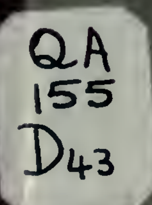


Dedekind, Richard
Uber die Anzhl der
Ideal-Classen



FESTSCHRIFT

ZUR

SAECULARFEIER DES GEBURTSTAGES

VON

CARL FRIEDRICH GAUSS

DARGEBRACHT

VOM

HERZOGLICHEN COLLEGIUM CAROLINUM

ZU

BRAUNSCHWEIG.

ÜBER DIE

ANZAHL DER IDEAL-CLASSEN

IN DEN

VERSCHIEDENEN ORDNUNGEN EINES ENDLICHEN KÖRPERS.

VON

RICHARD DEDEKIND.

BRAUNSCHWEIG,

DRUCK UND PAPIER VON FRIEDRICH VIEWEG UND SOHN.

1877.

FESTSCHRIFT

ZUR

SAECULARFEIER DES GEBURTSTAGES

VON

CARL FRIEDRICH GAUSS

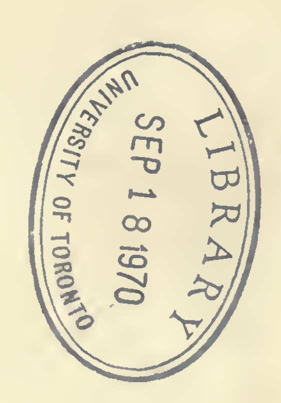
DARGEBRACHT

VOM

HERZOGLICHEN COLLEGIUM CAROLINUM

ZU

BRAUNSCHWEIG.


LIBRARY
SEP 18 1970
UNIVERSITY OF TORONTO

FESTSCHRIFT

ZUR

SAECULARFEIER DES GEBURTSTAGES

VON

CARL FRIEDRICH GAUSS

DARGEBRACHT

VOM

HERZOGLICHEN COLLEGIUM CAROLINUM

ZU

BRAUNSCHWEIG.

ÜBER DIE

ANZAHL DER IDEAL-CLASSEN

IN DEN

VERSCHIEDENEN ORDNUNGEN EINES ENDLICHEN KÖRPERS.

VON

RICHARD DEDEKIND.

BRAUNSCHWEIG,
DRUCK UND PAPIER VON FRIEDRICH VIEWEG UND SOHN.
1877.

DEM ANDENKEN

DES

MEISTERS DER MATHEMATISCHEN WISSENSCHAFTEN

CARL FRIEDRICH GAUSS

WIDMET

AM 30. APRIL 1877

ZUR

SAECULARFEIER SEINES GEBURTSTAGES

DAS

COLLEGIUM CAROLINUM,

DEM ER IN DEN JAHREN 1792 BIS 1795 ALS ZÖGLING ANGEHÖRT HAT,

DIESES ZEICHEN

DER

HULDIGUNG UND BEWUNDERUNG.

ÜBER DIE

ANZAHL DER IDEAL-CLASSEN

IN DEN

VERSCHIEDENEN ORDNUNGEN EINES ENDLICHEN KÖRPERS.

INHALT.

Die erhabenen Schöpfungen von Carl Friedrich Gauss haben die Bewunderung der Mathematiker dieses Jahrhunderts vor Allem deshalb erregt, weil sie in fast beispielloser Weise die Wissenschaft mit einer ausserordentlichen Fülle ganz neuer Gedanken befruchtet und vorher gänzlich unbekannte Felder zum ersten Male der Forschung erschlossen haben. Im höchsten Maasse gilt dies von Gauss' Entdeckungen im Gebiete der höheren Arithmetik, die ihn nach seinem eigenen Ausspruche das ganze Leben hindurch vor allen anderen Theilen der Mathematik gefesselt hat. Mit der Theorie der Kreistheilung ist von ihm nicht bloss der Grund zu einem neuen Theile der Mathematik gelegt, welcher von der algebraischen Verwandtschaft der Zahlen handelt, sondern sie hat auch das erste und bis jetzt noch immer fruchtbarste Beispiel des innigen Zusammenhangs zwischen der höheren Algebra und der Zahlentheorie geliefert, welche bis dahin zwei vollständig getrennte Gebiete gebildet hatten. In der nächsten Beziehung zu dieser Erweiterung der Grenzen der Wissenschaft steht der kühne Gedanke, den Begriff der ganzen Zahl durch die Einführung der ganzen complexen Zahlen von seiner bisherigen Beschränkung zu befreien, wodurch Gauss abermals der arithmetischen Forschung ein heute noch unermessliches Feld eröffnet hat. Aber es ist nicht bloss dieser wunderbare Reichthum an neuen Gedanken und grossen Entdeckungen, durch welchen Gauss sein Wirken auf allen von ihm beschrittenen Gebieten der Wissenschaft für alle Zeiten bezeichnet hat, sondern es steht diesem vollständig ebenbürtig die Tiefe der Methoden gegenüber, durch welche er die grössten Schwierigkeiten überwunden und die verborgensten Wahrheiten, die *mysteria numerorum*, in das hellste Licht gesetzt hat. Es genügte seinem stets auf das Grosse und auf die zukünftige Entwicklung

der Wissenschaft blickenden Geiste nicht, einen Beweis gefunden und damit die Wahrheit ausser Zweifel gesetzt zu haben, sondern er kehrte, wie er selbst so eindringlich beschreibt, unablässig zu den schon überwundenen Schwierigkeiten zurück, in der Hoffnung, durch erneute Anstrengungen neue Waffen zu gewinnen, welche eine über das unmittelbar vorliegende Ziel weit hinausreichende Tragweite besässen. Und so ist es gekommen, dass dieselben von Gauss erdachten Methoden unmittelbar oder mit geringen Modificationen auch bei der Behandlung von ähnlichen, aber allgemeineren Problemen sich als vollständig ausreichend erweisen. Diese schon oft als ein besonders charakteristisches Kennzeichen der Gedankentiefe von Gauss hervorgehobene Erscheinung an einem neuen Beispiele zu bestätigen, ist der Zweck der gegenwärtigen Abhandlung, welche dem Andenken des grossen Mathematikers gewidmet ist.

Die Theorie der binären quadratischen Formen, zu deren Entstehung einige Sätze von *Fermat* die Veranlassung gegeben haben, verdankt ihre Begründung den hervorragenden Arbeiten von *Euler* und *Lagrange,* aber sie ist erst von Gauss durch die in der fünften Section der Disquisitiones Arithmeticae niedergelegten Untersuchungen zu einem wissenschaftlichen Ganzen gestaltet, und namentlich hat sie durch die daselbst zum ersten Male behandelte Lehre von der Composition der Formen die höchste Bereicherung erhalten. Unter den Anwendungen, welche Gauss von dieser neuen Theorie gemacht hat, ist eine der bemerkenswerthesten die Bestimmung des *Verhältnisses* der Classen-Anzahlen der Formen, welche zu zwei verschiedenen *Ordnungen* derselben Determinante D gehören; bezeichnet man mit $h(D)$ die Classen-Anzahl für diejenige Ordnung der Determinante D, welche nur primitive Formen (und zwar entweder nur die eigentlichen oder nur die uneigentlichen) enthält, so kommt diese Aufgabe darauf hinaus, für zwei gegebene, in quadratischem Verhältniss stehende, Determinanten D und D' das Verhältniss $h(D) : h(D')$ zu ermitteln. Die aus der Theorie der Composition der Formen geschöpfte Beantwortung dieser Frage ist im Art. 256. V. und VI. enthalten, und sie ist für den Fall *negativer* Determinanten eine so vollständige, dass der Werth des Verhältnisses $h(D) : h(D')$ unmittelbar aus den Werthen von D und D' entnommen werden kann; nicht eben so vollständig durchgeführt ist der Fall *positiver* Determinanten, über welchen Gauss Folgendes sagt: *„Pro casu tertio autem, ubi D est numerus positivus non quadratus, regulam generalem pro comparanda multitudine formarum pr. primitivarum in V, V', V'' etc. cum multitudine classium diversarum inde resultantium hucusque non habe-*

mus. Id quidem asserere possumus, hanc vel illi aequalem vel ipsius partem aliquotam esse; quin etiam nexum singularem inter quotientem horum numerorum et valores minimos ipsorum t, u aequationi $tt - Duu = AA$ *satisfacientes deteximus, quem hic explicare nimis prolixum foret; an vero possibile sit, illum quotientem in omnibus casibus ex sola inspectione numerorum D, A cognoscere (ut in casibus praecc.), de hac re nihil certi pronunciare possumus.*"

Das umfassendere und noch viel schwierigere Problem, die Classen-Anzahl $h(D)$ *selbst*, d. h. die Abhängigkeit dieser Anzahl von der Determinante D zu bestimmen, ist schon während des Drucks der fünften Section der Disquisitiones Arithmeticae, wie aus Art. 306. X. hervorgeht, ein Gegenstand des höchsten Interesse für Gauss gewesen, und es ist ihm in der That bald darauf gelungen, die vollständige Lösung desselben zu finden, was er noch am Schlusse des grossen Werkes mit folgenden Worten ankündigen konnte: „*Quaestionem hic propositam plene solvere nuper successit, quam disquisitionem plures partes tum Arithmeticae sublimioris tum Analyseos mirifice illustrantem in continuatione hujus operis trademus quam primum licebit.*" Allein die hier in Aussicht gestellte Veröffentlichung dieser Untersuchung ist zu Gauss' Lebzeiten nicht erfolgt; der hierauf bezügliche Theil seines Nachlasses, welchen ich in dem 1863 erschienenen zweiten Bande seiner gesammelten Werke herausgegeben habe, enthält namentlich zwei Fragmente, die aus den Jahren 1834 und 1837 stammen und den gemeinsamen Titel führen „*De nexu inter multitudinem classium, in quas formae binariae secundi gradus distribuuntur, earumque determinantem.*" Obgleich jedes dieser Fragmente nach wenigen Seiten abbricht, so reicht ihr Inhalt doch aus, um den Weg vollständig überblicken zu lassen, auf welchem Gauss zu dem erstrebten Ziele gelangt ist.

Im Jahre 1839, also 38 Jahre nach dem Erscheinen der Disquisitiones Arithmeticae, trat *Peter Gustav Lejeune Dirichlet*, der nach Gauss' eigenem Zeugniss zuerst von allen Mathematikern dieses Werk vollständig begriffen und die darin enthaltenen Untersuchungen selbständig weiter geführt hat, mit einer vollständigen und höchst eigenthümlichen Lösung des Problems der Classen-Anzahl hervor*). Ohne hier, was zu weit führen würde, auf eine nähere Vergleichung der Methode von Dirichlet mit derjenigen von Gauss einzugehen, bemerke ich nur, dass von Beiden für die Classen-Anzahl ein Ausdruck durch eine unendliche Reihe gewonnen wird,

*) Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres (Crelle's Journal Bd. 19, 21).

welche sich mit Hülfe gewisser, der Kreistheilung angehörender Sätze von Gauss summiren, also in geschlossener Form darstellen lässt. Aber es ist von Wichtigkeit, dass es schon *vor* Ausführung dieser Summation gelingt, aus dem erhaltenen Ausdrucke den Werth des oben besprochenen *Verhältnisses* $h(D):h(D')$ abzuleiten. Auf diese Weise*) ist Dirichlet für den Fall negativer Determinanten zu demselben Resultate gelangt, wie Gauss, und er hat ausserdem für den Fall positiver Determinanten zum ersten Male das Gesetz vollständig ausgesprochen, nach welchem das gesuchte Verhältniss von den kleinsten Lösungen der unbestimmten Gleichungen $tt - Duu = 1$, $t't' - D'u'u' = 1$ abhängt. Aus der oben angeführten, auf diesen Fall bezüglichen Stelle der Disquisitiones Arithmeticae geht aber wohl mit Gewissheit hervor, dass Gauss ebenfalls dieses Gesetz schon vollständig gekannt hat, welches zwar einfach, aber doch keineswegs so einfach ist, dass man *ex sola inspectione numerorum* D, D' den Werth des gesuchten Verhältnisses erkennen könnte; auch habe ich gezeigt**), dass man wirklich auf dem von Gauss eingeschlagenen Wege, d. h. durch die Composition der Formen, mit wenigen Schritten zu diesem, zuerst von Dirichlet ausgesprochenen Gesetze gelangen kann.

Beide Methoden, das Verhältniss der Classen-Anzahlen zu bestimmen, sowohl die von Gauss, welche auf die Composition der Formen gegründet ist, als auch diejenige von Dirichlet, zeichnen sich nun dadurch aus, dass sie auf ähnliche Probleme von sehr allgemeinem Charakter mit demselben Erfolge anwendbar sind***). Die binären quadratischen Formen, von welchen bisher ausschliesslich gesprochen ist, bilden nämlich nur einen äusserst speciellen Fall der sogenannten *zerlegbaren Formen*, d. h. der homogenen Functionen von beliebig hohem Grade n mit n Variabelen, welche rationale Coefficienten haben und in n lineare Factoren mit *algebraischen* Coefficienten zerlegbar sind. Das Verdienst, diese Formen zuerst betrachtet und eine charakteristische Fundamental-Eigenschaft derselben erkannt zu haben, gebührt *Lagrange* †), und eine weitere Verfolgung seines Gedankens hätte leicht

---

*) Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres (Crelle's Journal Bd. 21, §. 8).

**) Vorlesungen über Zahlentheorie von P. G. Lejeune Dirichlet. Zweite Auflage. 1871. §§. 150, 151. — Ich werde dieses Werk in der Folge kurz mit D. citiren.

***) Ob Dasselbe auch von der scharfsinnigen Methode gilt, welche R. Lipschitz zur Lösung derselben Aufgabe angewandt hat (Crelle's Journal Bd. 53), wage ich für jetzt nicht zu beurtheilen; doch spricht dafür der Erfolg, mit welchem er diese Methode auf ein höheres Problem übertragen hat (Crelle's Journal Bd. 54).

†) Sur la solution des problèmes indéterminés du second degré. §. VI. Mém. de l'Ac. de Berlin. T. XXIII, 1769. — Élémens d'Algèbre par L. Euler; Additions §. IX.

schon früher zu der Theorie der Composition der Formen führen können. Erst viel später hat sich Dirichlet eingehend mit diesem Gegenstande beschäftigt; leider ist von seinen tiefen Untersuchungen — abgesehen von der ebenfalls hierher gehörigen, aber speciellen Theorie der quadratischen Formen mit complexen Coefficienten und Variabeln *) — nur eine einzige veröffentlicht, welche die Theorie der Transformation dieser Formen in sich selbst, oder anders ausgedrückt, die Theorie der *Einheiten* in dem entsprechenden Gebiete *algebraischer Zahlen* behandelt. Der in äusserst kurzen Umrissen von Dirichlet mitgetheilte Beweis **) für die Existenz und für die allgemeine Form aller dieser Einheiten, welcher ihm erst nach grossen und anhaltenden Anstrengungen gelungen ist, muss zu seinen bedeutendsten Leistungen gezählt werden, da derselbe ein unerlässliches Fundament für die ganze Theorie bildet; und Dirichlet selbst, der seinen eigenen Schöpfungen gegenüber sich immer ein ganz unbefangenes Urtheil bewahrte, legte auf dies Resultat einen eben so hohen Werth, wie auf die Principien, welche ihn zu dem Beweise des Satzes über die arithmetische Progression und zur Bestimmung der Classen-Anzahl der binären quadratischen Formen geführt haben. Dirichlet hat auch die Classen-Anzahl für solche zerlegbare Formen bestimmt, welche aus der Theorie der Kreistheilung entspringen, aber hiervon ist Nichts veröffentlicht ***). Es folgte zunächst im Jahre 1844 eine werthvolle Untersuchung von *Eisenstein* †) über gewisse cubische Formen, welche aus der Kreistheilung entspringen; doch scheint dieselbe wegen ihres sehr speciellen Charakters keinen bedeutenden Einfluss auf die Entwicklung der allgemeinen Theorie ausgeübt zu haben. Den grössten und folgenreichsten Schritt aber hat *Kummer* ††) im Jahre 1847 durch die Einführung der *idealen Zahlen* gethan; denn wenn auch seine Untersuchungen ebenfalls sich zunächst nur auf die Kreistheilung und einige derselben nahe stehende Gebiete beziehen, so sind doch die ihnen zu Grunde liegenden Gedanken von viel allgemeinerer Bedeutung. Der ausserordentliche, von Kummer erreichte Erfolg hat mich schon seit dem Jahre 1856 angetrieben, meine Kräfte hauptsächlich diesem Gegenstande zu widmen, und es ist mir endlich gelungen, eine allgemeine, ausnahmelose Theorie

---

*) Crelle's Journal Bd. 24.

**) Monatsberichte der Berliner Akademie vom October 1841, April 1842, März 1846. — Comptes rendus der Pariser Akademie 1840, T. X, p. 286.

***) Vergl. Kummer: Gedächtnissrede auf G. P. Lejeune Dirichlet, 1860, p. 21—22.

†) Crelle's Journal Bd. 28.

††) Crelle's Journal Bd. 35.

der ganzen algebraischen Zahlen aufzustellen, deren *Grundlagen* ich in dem zehnten Supplemente der zweiten Auflage von Dirichlet's Vorlesungen über Zahlentheorie veröffentlicht habe*). Mit Hülfe dieser Principien, welche ich hier als bekannt voraussetzen muss, lässt sich nun das auf die zerlegbaren Formen von beliebigem Grade oder auf die entsprechenden Ideal-Classen übertragene Problem, das Verhältniss der Classen-Anzahlen für verschiedene Ordnungen zu bestimmen, sowohl nach der Methode von Gauss, als auch nach derjenigen von Dirichlet vollständig lösen, und hierin besteht das Ziel der vorliegenden Abhandlung.

§. 1.

Theorie der ganzen Zahlen eines endlichen Körpers.

Obwohl diese Theorie, deren Mittelpunct die Lehre von der Multiplication der Ideale und von der Composition der Ideal-Classen bildet, hier als bekannt vorausgesetzt werden muss, so wird es doch zweckmässig sein, die wichtigsten ihr zu Grunde liegenden Begriffe hier möglichst kurz in Erinnerung zu bringen, schon um den Anknüpfungspunct der jetzigen Abhandlung an meine früheren Untersuchungen deutlicher hervorheben zu können.

Ist θ eine algebraische Zahl, und zwar eine Wurzel einer irreductibelen Gleichung

$$f(\theta) = \theta^n + a_1\,\theta^{n-1} + \cdots + a_{n-1}\,\theta + a_n = 0$$

vom n^{ten} Grade, deren Coefficienten $a_1, a_2 \cdots a_{n-1}, a_n$ rationale Zahlen sind, und betrachtet man die sämmtlichen Zahlen von der Form

$$\omega = \varphi(\theta) = x_0 + x_1\,\theta + x_2\,\theta^2 + \cdots + x_{n-1}\,\theta^{n-1},$$

wo $x_0, x_1, x_2 \cdots x_{n-1}$ willkürliche rationale Zahlen bedeuten, so besitzt der Inbegriff Ω aller dieser Zahlen ω die charakteristische Eigenschaft eines *Körpers* (D. §. 159), welche darin besteht, dass die Summen, Differenzen, Producte und Quotienten von je zwei solchen Zahlen ω ebenfalls in Ω enthalten sind; ein Körper Ω, dessen

*) Eine etwas ausführlichere Darstellung eines Theiles dieser Theorie erscheint gegenwärtig unter dem Titel *Sur la théorie des nombres entiers algébriques* in dem *Bulletin des sciences mathématiques et astronomiques* von *Darboux* und *Hoüel*. — Ich werde diese Abhandlung mit B. citiren.

Zahlen auf die angegebene Art aus einer Wurzel θ einer irreductibelen Gleichung n^{ten} Grades gebildet sind, heisst speciell ein *endlicher* Körper vom *Grade n.* Hat man n Zahlen

$$\omega_1 = \varphi_1(\theta),\ \omega_2 = \varphi_2(\theta) \cdots \omega_n = \varphi_n(\theta)$$

nach Belieben, nur mit der einzigen Beschränkung aus Ω ausgewählt, dass die aus den n^2 rationalen Coefficienten x gebildete Determinante einen von 0 verschiedenen Werth besitzt, so lässt sich jede beliebige Zahl ω des Körpers Ω stets und nur auf eine einzige Weise in der Form

$$\omega = h_1\,\omega_1 + h_2\,\omega_2 + \cdots + h_n\,\omega_n$$

darstellen, wo $h_1, h_2 \cdots h_n$ rationale Zahlen bedeuten. Ein solches System von n Zahlen $\omega_1, \omega_2 \cdots \omega_n$ heisst eine *Basis des Körpers* Ω, und die n rationalen Zahlen $h_1, h_2 \cdots h_n$ heissen die *Coordinaten der Zahl* ω in Bezug auf diese Basis. Offenbar bilden die Zahlen $1, \theta, \theta^2 \cdots \theta^{n-1}$ selbst eine solche Basis.

Ist θ' ebenfalls eine Wurzel derselben irreductibelen Gleichung $f(\theta') = 0$, so entspricht jeder bestimmten Zahl $\omega = \varphi(\theta)$ des Körpers Ω eine bestimmte Zahl $\omega' = \varphi(\theta')$, und der Inbegriff aller dieser Zahlen ω' bildet einen mit Ω *conjugirten Körper* Ω'; diese Correspondenz besitzt die charakteristische Eigenschaft, dass, wenn α, β zwei beliebige Zahlen des Körpers Ω bedeuten, stets

$$(\alpha+\beta)' = \alpha' + \beta',\ \ (\alpha-\beta)' = \alpha' - \beta',\ \ (\alpha\beta)' = \alpha'\beta',\ \ \left(\frac{\alpha}{\beta}\right)' = \frac{\alpha'}{\beta'}$$

ist; die Substitution, durch welche jede Zahl $\omega = \varphi(\theta)$ des Körpers Ω in die correspondirende oder *conjugirte Zahl* $\omega' = \varphi(\theta')$ des Körpers Ω' übergeht, heisse eine *Permutation des Körpers* Ω. Sind $\theta', \theta'' \cdots \theta^{(n)}$ die sämmtlichen Wurzeln der obigen irreductibelen Gleichung, so entspricht einer jeden von ihnen, $\theta^{(r)}$, eine Permutation $P^{(r)}$ des Körpers Ω, durch welche jede in ihm enthaltene Zahl $\omega = \varphi(\theta)$ in die conjugirte Zahl $\omega^{(r)} = \varphi(\theta^{(r)})$ des Körpers $\Omega^{(r)}$ übergeht. Die n mit ω conjugirten Zahlen $\omega', \omega'' \cdots \omega^{(n)}$ sind dann immer die Wurzeln einer Gleichung n^{ten} Grades mit rationalen Coefficienten, welche aber nicht nothwendig irreductibel ist. Das Product $\omega'\,\omega'' \cdots \omega^{(n)}$ aus diesen n Zahlen ist eine rationale Zahl, welche die *Norm der Zahl* ω heisst und mit $N(\omega)$ bezeichnet wird; sie verschwindet nur dann, wenn $\omega = 0$ ist, und die Norm eines Productes ist das Product aus den Normen der

Factoren. Sind ferner $\alpha_1, \alpha_2 \cdots \alpha_n$ beliebige Zahlen des Körpers, so ist das Quadrat der Determinante

$$\sum \pm \alpha_1' \alpha_2'' \cdots \alpha_n^{(n)},$$

welche aus den n^2 conjugirten Zahlen $\alpha_\iota^{(\iota)}$ gebildet ist, ebenfalls eine rationale Zahl, welche die *Discriminante des Systems* $\alpha_1, \alpha_2 \cdots \alpha_n$ heisst und mit $\Delta(\alpha_1, \alpha_2 \cdots \alpha_n)$ bezeichnet wird; dieselbe ist stets und nur dann von 0 verschieden, wenn die Zahlen $\alpha_1, \alpha_2 \cdots \alpha_n$ eine Basis des Körpers Ω bilden; dies ergiebt sich leicht aus dem bekannten Satze

$$\Delta\left(1, \theta, \theta^2 \cdots \theta^{n-1}\right) = (-1)^{\frac{1}{2}n(n-1)} N[f'(\theta)],$$

wo $f'(t)$ die Derivirte der Function $f(t)$ bedeutet. —

Alle algebraischen Zahlen, deren Gesammtheit ebenfalls einen Körper, aber keinen endlichen Körper bildet, zerfallen nun in ganze und in gebrochene Zahlen; eine algebraische Zahl η heisst eine *ganze Zahl,* wenn sie die Wurzel einer Gleichung von der Form

$$\eta^m + c_1 \eta^{m-1} + c_2 \eta^{m-2} + \cdots + c_{m-1} \eta + c_m = 0$$

ist, wo $c_1, c_2 \cdots c_{m-1}, c_m$ ganze Zahlen im alten Sinne des Wortes bedeuten, die von nun an immer *rationale ganze Zahlen* genannt werden sollen. Aus dieser Definition, welche wohl die höchste Verallgemeinerung des ursprünglich so beschränkten Begriffes der ganzen Zahl enthält, folgt unmittelbar, dass die Summen, Differenzen und Producte von je zwei ganzen Zahlen wieder ganze Zahlen sind, und hieran knüpft sich wieder der Begriff der *Theilbarkeit der ganzen Zahlen:* eine ganze Zahl α heisst *theilbar* durch eine ganze Zahl β, oder ein *Vielfaches (Multiplum)* von β, wenn $\alpha = \beta\gamma$, und γ wieder eine ganze Zahl ist; zugleich heisst γ ein *Theiler (Divisor)* von α, oder man sagt auch, β *gehe in* α *auf.* Eine ganze Zahl ε, welche in der Zahl 1 und folglich auch in allen ganzen Zahlen aufgeht, heisst eine *Einheit;* zwei ganze Zahlen, deren jede in der anderen aufgeht, und deren Quotient nothwendig eine Einheit ist, heissen *associirte Zahlen**) oder *Gefährten.* —

Kehrt man mit diesen allgemeinen Begriffen zu einem endlichen Körper Ω zurück, und bezeichnet man mit $\mathfrak{o}$ den Inbegriff *aller* in Ω enthaltenen ganzen

*) Vergl. Gauss: Theoria residuorum biquadraticorum II, Art. 31.

Zahlen, zu welchen auch alle ganzen rationalen Zahlen gehören, so ergiebt sich ohne Schwierigkeit die Existenz einer aus n ganzen Zahlen $\omega_1, \omega_2 \cdots \omega_n$ bestehenden Basis des Körpers Ω von der Beschaffenheit, dass die Coordinaten $h_1, h_2 \cdots h_n$ einer jeden in $\mathfrak{o}$ enthaltenen Zahl

$$\omega = h_1 \omega_1 + h_2 \omega_2 + \cdots + h_n \omega_n$$

ganze rationale Zahlen sind; die Discriminante

$$D = \Delta\,(\omega_1, \omega_2 \cdots \omega_n)$$

eines solchen Systems $\omega_1, \omega_2 \cdots \omega_n$, welches auch eine *Basis des Gebietes* $\mathfrak{o}$ heissen soll, ist eine ganze rationale, von 0 verschiedene Zahl, die ich ihrer Wichtigkeit wegen die *Grundzahl* oder die *Discriminante des Körpers* Ω nenne und mit $\Delta\,(\Omega)$ bezeichne. Die Norm einer jeden von 0 verschiedenen Zahl μ des Gebietes $\mathfrak{o}$ ist eine ganze rationale, von 0 verschiedene Zahl, welche die folgende, wichtige Bedeutung besitzt; nennt man zwei ganze Zahlen α, β *congruent* oder *incongruent* in Bezug auf den *Modulus* μ, je nachdem ihre Differenz $\alpha - \beta$ durch μ theilbar oder nicht theilbar ist, so ist die Anzahl aller in $\mathfrak{o}$ enthaltenen, nach μ incongruenten Zahlen $= \pm\, N(\mu)$; die Congruenz der Zahlen α, β in Bezug auf μ wird durch $\alpha \equiv \beta$ (mod. μ) bezeichnet. Eine in $\mathfrak{o}$ enthaltene Einheit ist dadurch charakterisirt, dass ihre Norm $= \pm 1$ ist.

Die wichtigste Frage ist aber die nach der Zerlegung einer in $\mathfrak{o}$ enthaltenen Zahl μ in solche Factoren, welche, wie im Folgenden immer stillschweigend vorausgesetzt wird, ebenfalls dem Gebiete $\mathfrak{o}$ angehören. Die Divisoren einer Einheit sind sämmtlich selbst Einheiten; ist aber μ keine Einheit, so sind zwei Fälle möglich; ist μ das Product aus zwei Factoren, von denen keiner eine Einheit, und folglich auch keiner mit μ associirt ist, so soll μ eine *zerlegbare Zahl* heissen; im entgegengesetzten Fall, d. h. wenn jeder Divisor von μ entweder ein Gefährte von μ oder eine Einheit ist, heisst μ *unzerlegbar*. Aus dem Satze über die Norm eines Productes folgt nun offenbar, dass jede zerlegbare Zahl stets als Product aus einer endlichen Anzahl von unzerlegbaren Factoren darstellbar ist; während aber in der Theorie der rationalen Zahlen (d. h. im Falle $n = 1$) diese Zerlegung, abgesehen von den Einheits-Factoren ± 1, eine völlig bestimmte, einzige ist, so tritt bei Körpern höheren Grades sehr häufig die merkwürdige Erscheinung auf, dass eine Zahl μ als Product von unzerlegbaren Factoren auf mehrere Arten darstellbar ist,

welche in dem Sinne wesentlich verschieden sind, dass z. B. ein unzerlegbarer Factor α der einen Darstellung $\mu = \alpha\beta\gamma\cdots$ mit keinem der unzerlegbaren Factoren $\alpha_1, \beta_1 \cdots$ der anderen Darstellung $\mu = \alpha_1\beta_1\cdots$ associirt ist. Es folgt hieraus, dass eine unzerlegbare Zahl durchaus nicht immer den Charakter einer eigentlichen *Primzahl* besitzt, welcher darin besteht, dass ein Product nur dann durch eine Primzahl theilbar ist, wenn diese wenigstens in einem der Factoren aufgeht. Diese unwillkommene Erscheinung, welche auf den ersten Blick jeden weiteren Fortschritt auf diesem Felde zu verbieten schien, ist aber die Quelle von einer der schönsten und fruchtbarsten Entdeckungen in der höheren Arithmetik geworden: in der That ist *Kummer* bei der Untersuchung solcher Gebiete $\mathfrak{o}$, welche aus der *Kreistheilung* entspringen, dahin gelangt, die Gesetze der Theilbarkeit durch Einführung *idealer Zahlen* in völligen Einklang mit denjenigen zu bringen, welche in der alten Theorie der rationalen Zahlen herrschen.

Es ist das Ziel meiner langjährigen Bemühungen gewesen, dasselbe Resultat für *jeden endlichen Körper* Ω zu erreichen, also diejenigen allgemeinen Gesetze der Theilbarkeit festzustellen, welche ohne Ausnahme *jedem Gebiete* $\mathfrak{o}$ von der oben beschriebenen Art zukommen. Bei der Begründung dieser Theorie (D. §. 163) habe ich den von Kummer eingeschlagenen Weg verlassen und statt der *idealen Zahlen* einen anderen Begriff, den des *Ideals*, einführen müssen, welcher von jeder, einem speciellen Körper Ω eigenthümlichen Färbung frei ist und gerade deshalb die erforderliche Allgemeinheit besitzt, um als Grundlage der Theorie dienen zu können. Zum Verständnisse der nachfolgenden Untersuchungen ist es unerlässlich, an die Hauptsätze dieser Theorie kurz zu erinnern.

1°. Ein System $\mathfrak{m}$ von unendlich vielen Zahlen des Gebietes $\mathfrak{o}$ heisst ein *Ideal*, wenn es die beiden folgenden Eigenschaften besitzt:

I. Die Summen und Differenzen von je zwei Zahlen des Systems $\mathfrak{m}$ sind ebenfalls in $\mathfrak{m}$ enthalten.

II. Jedes Product aus einer Zahl des Systems $\mathfrak{m}$ und aus einer Zahl des Systems $\mathfrak{o}$ ist eine Zahl des Systems $\mathfrak{m}$.

Bedeutet μ eine bestimmte, ω jede beliebige Zahl in $\mathfrak{o}$, so kommen diese beiden Eigenschaften offenbar dem System $\mathfrak{m}$ aller durch μ theilbaren Zahlen $\mu\omega$ zu; ein solches Ideal $\mathfrak{m}$ heisst ein *Hauptideal* und wird mit $\mathfrak{o}(\mu)$ oder kürzer mit $\mathfrak{o}\mu$ oder $\mu\mathfrak{o}$ bezeichnet*); es bleibt ungeändert, wenn μ durch eine mit μ asso-

*) Früher habe ich die weniger zweckmässige Bezeichnung $\mathfrak{i}(\mu)$ angewendet (D. §. 163).

ciirte Zahl ersetzt wird. Ist μ eine Einheit, so ist $\mathfrak{o}\mu = \mathfrak{o}$, und umgekehrt. Da die Congruenz zweier Zahlen α, β in Bezug auf den Modulus μ darin besteht, dass die Differenz $\alpha - \beta$ dem Ideal $\mathfrak{o}\mu$ angehört, so wird man zu der folgenden allgemeineren Definition der Congruenz geführt:

2⁰. Zwei Zahlen α, β heissen *congruent in Bezug auf ein Ideal* $\mathfrak{m}$, und dies wird durch die Congruenz $\alpha \equiv \beta \pmod{\mathfrak{m}}$ angedeutet, wenn $\alpha - \beta$ eine Zahl des Ideals $\mathfrak{m}$ ist; im entgegengesetzten Falle heissen α, β *incongruent* nach $\mathfrak{m}$. Die immer endliche Anzahl aller in $\mathfrak{o}$ enthaltenen, in Bezug auf $\mathfrak{m}$ incongruenten Zahlen heisst die *Norm des Ideals* $\mathfrak{m}$ und wird mit $N(\mathfrak{m})$ bezeichnet; die Norm eines Hauptideals $\mathfrak{o}\mu$ ist $= \pm N(\mu)$; das Hauptideal $\mathfrak{o}$ ist das einzige Ideal, dessen Norm $= 1$ ist.

Die Theilbarkeit einer Zahl $\mu = \alpha\beta$ durch eine Zahl α besteht darin, dass alle Zahlen $\mu\omega = \alpha(\beta\omega)$ des Ideals $\mathfrak{o}\mu$ auch in dem Ideale $\mathfrak{o}\alpha$ enthalten sind; dies veranlasst zu der folgenden Definition der *Theilbarkeit der Ideale:*

3⁰. Ein Ideal $\mathfrak{m}$ heisst *theilbar* durch ein Ideal $\mathfrak{a}$ oder ein *Vielfaches* von $\mathfrak{a}$, wenn alle Zahlen des Ideals $\mathfrak{m}$ auch dem Ideale $\mathfrak{a}$ angehören; zugleich heisst $\mathfrak{a}$ ein *Theiler* von $\mathfrak{m}$, oder man sagt auch, $\mathfrak{a}$ *gehe in* $\mathfrak{m}$ *auf.*

Da hiernach die Theilbarkeit der *Zahlen* nur einen speciellen Fall von der Theilbarkeit der *Ideale* bildet, so kommt es lediglich darauf an, die thatsächlich *einfacheren* Gesetze der letzteren festzustellen. Dies geschieht durch die folgenden Begriffe und Sätze:

4⁰. Ist das Ideal $\mathfrak{m}$ theilbar durch das Ideal $\mathfrak{a}$, und letzteres theilbar durch das Ideal $\mathfrak{d}$, so ist auch $\mathfrak{m}$ theilbar durch $\mathfrak{d}$.

5⁰. Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei beliebige Ideale, so bildet das System $\mathfrak{m}$ aller den Idealen $\mathfrak{a}$, $\mathfrak{b}$ gemeinschaftlich angehörenden Zahlen ein Ideal, welches das *kleinste gemeinschaftliche Vielfache* von $\mathfrak{a}$, $\mathfrak{b}$ heisst, weil es in jedem gemeinschaftlichen Vielfachen von $\mathfrak{a}$, $\mathfrak{b}$ aufgeht.

6⁰. Durchläuft α alle Zahlen eines Ideals $\mathfrak{a}$, ebenso β alle Zahlen eines Ideals $\mathfrak{b}$, so bildet das System $\mathfrak{d}$ aller in der Form $\alpha + \beta$ darstellbaren Zahlen ein Ideal, welches der *grösste gemeinschaftliche Theiler* von $\mathfrak{a}$, $\mathfrak{b}$ heisst, weil jeder gemeinschaftliche Theiler von $\mathfrak{a}$, $\mathfrak{b}$ in dem Ideal $\mathfrak{d}$ aufgeht.

7⁰. Zwei Ideale, deren grösster gemeinschaftlicher Theiler das Ideal $\mathfrak{o}$ ist, heissen *relative Primideale.*

8⁰. Ein von $\mathfrak{o}$ verschiedenes Ideal $\mathfrak{p}$ heisst ein *Primideal,* wenn es kein von

$\mathfrak{o}$ und $\mathfrak{p}$ verschiedenes Ideal zum Theiler hat; im entgegengesetzten Falle heisst $\mathfrak{p}$ ein *zusammengesetztes* Ideal.

9°. Durchläuft α alle Zahlen eines Ideals $\mathfrak{a}$, ebenso β alle Zahlen eines Ideals $\mathfrak{b}$, so bilden die sämmtlichen Producte $\alpha\beta$ und alle Summen von solchen Producten ein durch $\mathfrak{a}$ und durch $\mathfrak{b}$ theilbares Ideal, welches das *Product* aus den *Factoren* $\mathfrak{a}$ und $\mathfrak{b}$ heisst und mit $\mathfrak{ab} = \mathfrak{ba}$ bezeichnet wird; zugleich ist $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$. Die Ausdehnung dieses Begriffes auf beliebig viele Factoren und die Bedeutung einer *Potenz* ist selbstverständlich.

10°. Umgekehrt: ist das Ideal $\mathfrak{m}$ theilbar durch das Ideal $\mathfrak{a}$, so giebt es ein und nur ein Ideal $\mathfrak{b}$ von der Art, dass $\mathfrak{ab} = \mathfrak{m}$ wird.

11°. Ein Product von Idealen ist nur dann durch ein Primideal theilbar, wenn dieses wenigstens in einem der Factoren aufgeht.

12°. Jedes zusammengesetzte Ideal ist als Product von lauter Primidealen darstellbar, und zwar nur auf eine einzige Weise.

13°. Damit ein Ideal $\mathfrak{m}$ durch ein Ideal $\mathfrak{a}$ theilbar sei, ist erforderlich und hinreichend, dass alle in $\mathfrak{a}$ aufgehenden Potenzen von Primidealen auch in $\mathfrak{m}$ aufgehen.

14°. Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei beliebige Ideale, so giebt es ein durch $\mathfrak{a}$ theilbares Hauptideal $\mathfrak{am}$ von der Art, dass $\mathfrak{m}$ und $\mathfrak{b}$ relative Primideale werden.

Für den Fall $n = 1$, in welchem alle Ideale Hauptideale sind, gehen die vorstehenden Sätze, deren strenge Beweise mir erst nach Ueberwindung von erheblichen Schwierigkeiten gelungen sind, in die Fundamentalsätze über die Theilbarkeit der ganzen rationalen Zahlen über. Dieselben Gesetze gelten daher auch für jeden Körper Ω von beliebigem Grade n, sobald alle seine Ideale Hauptideale sind, und für einen solchen Körper ist offenbar die Einführung der Ideale gänzlich überflüssig. Dies ist aber, wie schon oben bemerkt, im Allgemeinen keineswegs der Fall, und hieran knüpft sich die Eintheilung aller Ideale eines Körpers Ω in bestimmte *Ideal-Classen* (D. §. 164). Zwei Ideale $\mathfrak{a}$, $\mathfrak{b}$ heissen *äquivalent*, wenn es ein Ideal $\mathfrak{c}$ giebt, für welches beide Producte $\mathfrak{ac}$, $\mathfrak{bc}$ Hauptideale werden; da aus dieser Definition unmittelbar folgt, dass zwei mit einem dritten äquivalente Ideale auch mit einander äquivalent sind, so bildet das System A aller Ideale, welche einem bestimmten Ideale $\mathfrak{a}$ äquivalent sind, eine *Classe*, welche ungeändert bleibt, wenn ihr *Repräsentant* $\mathfrak{a}$ durch ein beliebiges, derselben Classe A angehörendes Ideal ersetzt wird. Die *Anzahl* h dieser Classen ist immer eine *endliche;* wählt man

aus jeder Classe nach Belieben ein bestimmtes Ideal als Repräsentanten, so ist jedes Ideal mit einem und nur mit einem dieser h Ideale äquivalent. Das System aller Hauptideale bildet die *Hauptclasse O;* zu jeder Classe A von Idealen $\mathfrak{a}$ gehört eine bestimmte *entgegengesetzte* oder *reciproke, inverse* Classe A^{-1}, welche aus allen denjenigen Idealen besteht, die durch Multiplication mit den Idealen $\mathfrak{a}$ in Hauptideale verwandelt werden. Durchläuft nun $\mathfrak{a}$ alle Ideale einer Classe A, ebenso $\mathfrak{b}$ alle Ideale einer Classe B, so gehören die sämmtlichen Producte $\mathfrak{a}\mathfrak{b}$ einer und derselben Classe an, welche die *aus A und B zusammengesetzte Classe* oder das *Product* aus A, B heisst und mit AB bezeichnet wird; diese *Composition* oder *Multiplication der Ideal-Classen* gehorcht den Gesetzen $AB = BA$, $(AB)C = A(BC)$, $OA = A$, $AA^{-1} = O$, $A^r A^s = A^{r+s}$, $A^h = O$, und aus $AB = AC$ folgt $B = C$.

Aus dem Satze $A^h = O$ folgt beiläufig, wenn man von dem endlichen Körper Ω wieder zu dem Gebiete *aller* ganzen algebraischen Zahlen übergeht, das wichtige Resultat, dass je zwei ganze Zahlen α, β, die nicht beide verschwinden, einen *grössten* gemeinschaftlichen Divisor δ besitzen, welcher in der Form $\delta = \alpha\alpha_1 + \beta\beta_1$ darstellbar ist, wo α_1, β_1 ebenfalls ganze Zahlen bedeuten; natürlich kann auch hier δ durch jeden Gefährten von δ ersetzt werden.

Das grösste Interesse nimmt aber die *Bestimmung der Classen-Anzahl h* in Anspruch (D. §. 167). Die Uebertragung der Principien, welche Dirichlet bei dem Beweise des Satzes über die arithmetische Progression und bei der Bestimmung der Classen-Anzahl der binären quadratischen Formen geschaffen hat, führt zu der Betrachtung unendlicher Reihen und Producte von der Form

$$\sum f(\mathfrak{a}) = \prod \frac{1}{1 - f(\mathfrak{p})},$$

wo $\mathfrak{a}$ alle Ideale, $\mathfrak{p}$ alle Primideale durchläuft, und $f(\mathfrak{a})$ eine reelle oder complexe Function bedeutet, die der Bedingung $f(\mathfrak{a}\mathfrak{b}) = f(\mathfrak{a})f(\mathfrak{b})$ genügt und ausserdem so beschaffen ist, dass die unendliche Reihe linker Hand eine von der Anordnung ihrer Glieder unabhängige endliche Summe besitzt. Diese Bedingungen sind erfüllt, wenn man

$$f(\mathfrak{a}) = \frac{1}{N(\mathfrak{a})^s}, \quad s > 1$$

nimmt; multiplicirt man mit $(s - 1)$ und theilt die Totalsumme in h Partialsummen,

deren jede einer bestimmten Classe von Idealen $\mathfrak{a}$ entspricht, so nähern sich diese Summen für unendlich kleine positive Werthe von $(s-1)$ einem *gemeinschaftlichen*, endlichen, von 0 verschiedenen Grenzwerth g, der sich nach den fundamentalen Untersuchungen Dirichlet's über die Einheiten ohne Schwierigkeit bestimmen lässt, und man erhält folglich

$$g\,h = \lim \sum \frac{s-1}{N(\mathfrak{a})^s} = \lim\,(s-1) \prod \frac{1}{1-\frac{1}{N(\mathfrak{p})^s}}.$$

Das Problem der Classen-Anzahl wird daher gelöst sein, sobald es gelingt, den Grenzwerth der unendlichen Reihe oder des mit ihr identischen Productes noch auf eine zweite Art, nämlich unmittelbar aus der Natur der sämmtlichen, dem Körper Ω angehörenden Primideale $\mathfrak{p}$ zu bestimmen. Dies ist bis jetzt nur für Kreistheilungs-Körper geglückt (zu welchen auch alle quadratischen Körper gehören), und eine aufmerksame Betrachtung dieser Fälle führt zu der Ueberzeugung — in welcher ich durch meine demnächst zu veröffentlichenden Untersuchungen über die Anzahl der Ideal-Classen in cubischen Körpern bestärkt werde —, dass die *allgemeine* Lösung des Problems der Classen-Anzahl auf diesem Wege erst dann gelingen wird, wenn die algebraische Constitution eines jeden Körpers und ihr Zusammenhang mit seinen Idealen uns vollständig bekannt sein wird — ein Ziel, von welchem wir noch ausserordentlich weit entfernt sind; ausserdem scheint auch eine viel genauere Ausbildung der Theorie der transcendenten Functionen erforderlich zu sein.

Es ist nun noch mit einigen Worten die Beziehung zwischen den Idealen eines Körpers und den zugehörigen *zerlegbaren Formen* zu besprechen (D. §. 165). Ist $\mathfrak{a}$ ein bestimmtes Ideal, so giebt es immer n particuläre, in $\mathfrak{a}$ enthaltene Zahlen $\alpha_1, \alpha_2 \cdots \alpha_n$ von der Beschaffenheit, dass die sämmtlichen Zahlen α des Ideals $\mathfrak{a}$ durch den Ausdruck

$$\alpha = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n$$

dargestellt werden, wenn die Variabelen $x_1, x_2 \cdots x_n$ alle ganzen rationalen Zahlen durchlaufen. Das System der Zahlen $\alpha_1, \alpha_2 \cdots \alpha_n$ heisst eine *Basis von* $\mathfrak{a}$. Bildet man das Product aus allen n mit α conjugirten Ausdrücken, so erhält man

$$N(\alpha) = N(\mathfrak{a})\,X,$$

wo X eine homogene Function n^{ten} Grades von den Variabelen $x_1, x_2 \cdots x_n$ bedeutet; die Coefficienten dieser zerlegbaren Form X sind immer ganze rationale Zahlen ohne gemeinschaftlichen Theiler. Da das Ideal $\mathfrak{a}$ unendlich viele verschiedene Basen besitzt, so entspricht demselben eine *Classe* von unendlich vielen *äquivalenten* Formen X, welche durch lineare Substitutionen mit ganzen rationalen Coefficienten gegenseitig in einander übergehen. Dieselben Formen entspringen aber auch aus jedem mit $\mathfrak{a}$ äquivalenten Ideal, und folglich entspricht jeder Ideal-Classe eine bestimmte Formen-Classe. Die Multiplication der Ideale und der Ideal-Classen führt zu der Composition der Formen und der Formen-Classen.

Aber diese Formen X umfassen nur einen unendlich kleinen Theil aller möglichen zu dem Körper Ω gehörenden Formen. Versteht man nämlich unter der *Determinante* einer aus n homogenen linearen Factoren $f_1, f_2 \cdots f_n$ gebildeten Function F von n Variabelen $h_1, h_2 \cdots h_n$ das Quadrat der Functional-Determinante

$$\sum \pm \frac{\partial f_1}{\partial h_1} \frac{\partial f_2}{\partial h_2} \cdots \frac{\partial f_n}{\partial h_n},$$

so ergiebt sich leicht, dass die Determinante aller oben betrachteten Formen X mit der Grundzahl $D = \Delta(\Omega)$ des Körpers Ω übereinstimmt; für den Fall $n = 2$ würde man z. B. nur zu solchen binären Formen $ax^2 + bxy + cy^2$ gelangen, deren Determinante $b^2 - 4ac = D$ durch kein ungerades Quadrat theilbar und entweder $\equiv 1$ (mod. 4), oder $\equiv 8, 12$ (mod. 16) ist*).

Um nun eine allgemeinere Theorie der zu einem Körper Ω gehörenden Formen aufzustellen, muss man, wie ich schon früher bemerkt habe (D. §. 165), den Begriff des Ideals so erweitern, dass an Stelle des bisher betrachteten Gebietes $\mathfrak{o}$, welches *alle* ganzen Zahlen des Körpers umfasst, beschränktere Gebiete $\mathfrak{o}'$ treten, welche ich mit Rücksicht auf die in der Theorie der binären quadratischen Formen von Gauss gebrauchte Ausdrucksweise *Ordnungen* genannt habe. Diese Erweiterung bildet den nächsten Gegenstand dieser Abhandlung.

---

*) Die obige Erklärung einer Formen-Determinante stimmt für den Fall $n = 2$ nicht ganz mit derjenigen von Gauss überein; dies lässt sich aber kaum vermeiden, wenn sie allgemein für jeden Grad n gelten soll, und selbst in dem speciellen Falle $n = 2$ sprechen viele Erscheinungen zu Gunsten derselben, was ich aber hier nicht näher begründen kann.

§. 2.

Sätze aus der Theorie der Moduln.

Um hierzu zu gelangen, und namentlich um beständige Wiederholungen über die Art zu vermeiden, in welcher aus gewissen Systemen von Zahlen neue Systeme gebildet werden, ist es nothwendig, hier einige sehr einfache und zugleich sehr allgemeine Sätze über solche Systeme einzuschalten, die ich *Moduln* genannt habe (D. §. 161). Da der Begriff eines Ideals in demjenigen eines Moduls als specieller Fall enthalten ist, so wird bei einer systematischen Darstellung die Theorie der Moduln zweckmässig der Theorie der Ideale voraufgeschickt werden. Hier wird es genügen, einige Hauptbegriffe zu entwickeln und einige Sätze anzuführen, deren Beweise ich unterdrücke, weil Jeder sie leicht finden wird (vergl. D. §. 161 und B. §§. 1 bis 4). Da manche dieser Sätze sich in Worten nur ziemlich umständlich aussprechen lassen, so wage ich es, die Ausdrucksweise durch Einführung einer Zeichensprache abzukürzen, und ich hoffe, dass man aus diesem Grunde die Benutzung der Zeichen $>$, $<$, $+$, $-$ entschuldigen wird. Ich bemerke nur noch, dass im Folgenden die Einschränkung auf die Zahlen eines endlichen Körpers gänzlich wegfällt, also das Wort *Zahl* immer in seiner allgemeinsten Bedeutung gebraucht wird.

1°. Ein System $\mathfrak{m}$ von reellen oder complexen Zahlen heisst ein *Modul*, wenn alle Summen und Differenzen dieser Zahlen demselben System $\mathfrak{m}$ angehören. Die Zahl 0 findet sich in jedem Modul, und sie bildet auch für sich allein einen Modul. Ein Modul $\mathfrak{m}$ heisst *theilbar* durch einen Modul $\mathfrak{a}$ oder ein *Vielfaches* von $\mathfrak{a}$, wenn alle Zahlen des Moduls $\mathfrak{m}$ auch in $\mathfrak{a}$ enthalten sind; zugleich heisst $\mathfrak{a}$ ein *Theiler* von $\mathfrak{m}$, und wir bezeichnen die Theilbarkeit von $\mathfrak{m}$ durch $\mathfrak{a}$ sowohl durch $\mathfrak{m} > \mathfrak{a}$, als durch $\mathfrak{a} < \mathfrak{m}$. Ist jeder der beiden Moduln $\mathfrak{m}$, $\mathfrak{a}$ durch den andern theilbar, so sind sie identisch, was durch $\mathfrak{m} = \mathfrak{a}$ angedeutet wird. Aus $\mathfrak{m} > \mathfrak{a}$, $\mathfrak{a} > \mathfrak{b}$ folgt $\mathfrak{m} > \mathfrak{b}$. Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei beliebige Moduln, so ist das System aller derjenigen Zahlen, welche beiden Moduln gemeinschaftlich angehören, selbst ein Modul und zwar ein Vielfaches von $\mathfrak{a}$ und von $\mathfrak{b}$, welches durch $\mathfrak{a} - \mathfrak{b} = \mathfrak{b} - \mathfrak{a}$ bezeichnet werden soll; dasselbe heisst das *kleinste gemeinschaftliche Vielfache von* $\mathfrak{a}$, $\mathfrak{b}$, weil jedes gemeinschaftliche Vielfache von $\mathfrak{a}$, $\mathfrak{b}$ durch $\mathfrak{a} - \mathfrak{b}$ theilbar ist. Durch-

läuft α alle Zahlen eines Moduls $\mathfrak{a}$, ebenso β alle Zahlen eines Moduls $\mathfrak{b}$, so ist das System aller Zahlen von der Form $\alpha + \beta$ ein Modul, und zwar ein Theiler von $\mathfrak{a}$ und von $\mathfrak{b}$, der mit $\mathfrak{a} + \mathfrak{b} = \mathfrak{b} + \mathfrak{a}$ bezeichnet werden soll; derselbe heisst der *grösste gemeinschaftliche Theiler von* $\mathfrak{a}, \mathfrak{b}$, weil jeder gemeinschaftliche Theiler von $\mathfrak{a}, \mathfrak{b}$ auch ein Theiler von $\mathfrak{a} + \mathfrak{b}$ ist. Diese Begriffe lassen sich leicht auf beliebig viele, sogar auf unendlich viele Moduln $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \cdots$ ausdehnen, und man beweist leicht die beiden folgenden charakteristischen Sätze

$$(\mathfrak{a} + \mathfrak{b}) - (\mathfrak{a} + \mathfrak{c}) = \mathfrak{a} + (\mathfrak{b} - (\mathfrak{a} + \mathfrak{c}))$$
$$(\mathfrak{a} - \mathfrak{b}) + (\mathfrak{a} - \mathfrak{c}) = \mathfrak{a} - (\mathfrak{b} + (\mathfrak{a} - \mathfrak{c})),$$

in welchen sich der zwischen den Begriffen des kleinsten gemeinschaftlichen Vielfachen und des grössten gemeinschaftlichen Theilers durchgängig herrschende Dualismus kundgiebt.

2^0. Zwei Zahlen α, β heissen *congruent* oder *incongruent in Bezug auf einen Modul* $\mathfrak{m}$, je nachdem ihre Differenz $\alpha - \beta$ in $\mathfrak{m}$ enthalten ist oder nicht; die Congruenz wird durch $\alpha \equiv \beta \pmod{\mathfrak{m}}$ ausgedrückt. Alle mit einer bestimmten Zahl nach $\mathfrak{m}$ congruenten Zahlen bilden eine *Zahl-Classe* (mod. $\mathfrak{m}$). Mehrere Zahlen heissen incongruent (mod. $\mathfrak{m}$), wenn jede derselben mit jeder der übrigen incongruent (mod. $\mathfrak{m}$) ist. Sind $\mathfrak{a}, \mathfrak{b}$ zwei beliebige Moduln, so kann es sein, dass $\mathfrak{a}$ nur eine endliche Anzahl incongruenter Zahlen in Bezug auf $\mathfrak{b}$ enthält, und dann soll diese Anzahl durch das Symbol $(\mathfrak{a}, \mathfrak{b})$ bezeichnet werden; giebt es aber in $\mathfrak{a}$ unendlich viele, in Bezug auf $\mathfrak{b}$ incongruente Zahlen, so soll $(\mathfrak{a}, \mathfrak{b}) = 0$ gesetzt werden, weil dann gewisse Determinanten-Sätze allgemein gültig bleiben. In beiden Fällen ist

$$(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{a}, \mathfrak{a} - \mathfrak{b}) = (\mathfrak{a} + \mathfrak{b}, \mathfrak{b});$$

ist $\mathfrak{a} > \mathfrak{b}$, so ist $(\mathfrak{a}, \mathfrak{b}) = 1$, und umgekehrt. Ist ferner $\mathfrak{m} > \mathfrak{a} > \mathfrak{b}$, so ist

$$(\mathfrak{b}, \mathfrak{m}) = (\mathfrak{b}, \mathfrak{a})\,(\mathfrak{a}, \mathfrak{m}).$$

Durch Combination beider Sätze erhält man viele andere Sätze, die hier übergangen werden können. Sind ρ, σ zwei gegebene Zahlen, so hat das System der beiden Congruenzen

$$\omega \equiv \rho \pmod{\mathfrak{a}}, \quad \omega \equiv \sigma \pmod{\mathfrak{b}}$$

stets und nur dann gemeinschaftliche Wurzeln ω, wenn

$$\rho \equiv \sigma \pmod{\mathfrak{a} + \mathfrak{b}}$$

ist, und die sämmtlichen Zahlen ω bilden eine bestimmte Zahlclasse (mod. $\mathfrak{a} - \mathfrak{b}$).

3⁰. Sind $\alpha_1, \alpha_2 \cdots \alpha_n$ Constanten, während $x_1, x_2 \cdots x_n$ alle ganzen rationalen Zahlen durchlaufen, so bilden die sämmtlichen, in der Form

$$\alpha = x_1 \alpha_1 + x_2 \alpha_2 + \cdots + x_n \alpha_n$$

darstellbaren Zahlen α einen Modul $\mathfrak{a}$, der ein *endlicher Modul* heissen und mit $[\alpha_1, \alpha_2 \cdots \alpha_n]$ bezeichnet werden soll; die Constanten $\alpha_1, \alpha_2 \cdots \alpha_n$ bilden eine *Basis des Moduls* $\mathfrak{a}$. Der Modul [1] ist das System aller ganzen rationalen Zahlen. Wenn alle Zahlen eines solchen endlichen Moduls $\mathfrak{a} = [\alpha_1, \alpha_2 \cdots \alpha_n]$ durch Multiplication mit rationalen, von 0 verschiedenen Zahlen in Zahlen eines Moduls $\mathfrak{b}$ verwandelt werden können, so ist $(\mathfrak{a}, \mathfrak{b})$ von 0 verschieden, und $\mathfrak{a} - \mathfrak{b}$ ist ein endlicher Modul; man kann die ganzen rationalen Zahlen a so wählen, dass die n Zahlen

$$\begin{aligned}
\mu_1 &= a'_1 \alpha_1 \\
\mu_2 &= a''_1 \alpha_1 + a''_2 \alpha_2 \\
\mu_3 &= a'''_1 \alpha_1 + a'''_2 \alpha_2 + a'''_3 \alpha_3 \\
&\cdots\cdots\cdots \\
\mu_n &= a^{(n)}_1 \alpha_1 + a^{(n)}_2 \alpha_2 + a^{(n)}_3 \alpha_3 + \cdots + a^{(n)}_n \alpha_n
\end{aligned}$$

eine Basis von $\mathfrak{a} - \mathfrak{b}$ bilden, und dass zugleich

$$(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{a}, \mathfrak{a} - \mathfrak{b}) = a'_1 a''_2 a'''_3 \cdots a^{(n)}_n$$

wird; unterwirft man die n ganzen rationalen Zahlen $x'_1, x'_2 \cdots x'_n$ den n Bedingungen

$$0 \leqq x'_r < a^{(r)}_r,$$

so sind die entsprechenden, in $\mathfrak{a}$ enthaltenen Zahlen

$$\alpha' = x'_1 \alpha_1 + x'_2 \alpha_2 + \cdots + x'_n \alpha_n,$$

deren Anzahl $= (\mathfrak{a}, \mathfrak{b})$ ist, sämmtlich incongruent (mod. $\mathfrak{b}$) und deshalb auch incongruent (mod. $\mathfrak{a} - \mathfrak{b}$).

4⁰. Ein System von n Zahlen $\alpha_1, \alpha_2 \cdots \alpha_n$ soll ein *irreductibeles* System, und diese Zahlen sollen von einander *unabhängig* heissen, wenn die Summe

$$\alpha = x_1 \alpha_1 + x_2 \alpha_2 + \cdots + x_n \alpha_n$$

für jedes System von rationalen, nicht sämmtlich verschwindenden Zahlen $x_1, x_2 \cdots x_n$

einen von 0 verschiedenen Werth erhält. Ist nun wieder $\mathfrak{a} = [\alpha_1, \alpha_2 \ldots \alpha_n]$, und sind die Basiszahlen eines Moduls $\mathfrak{m} = [\mu_1, \mu_2 \cdots \mu_n]$ von der Form

$$\begin{aligned}
\mu_1 &= a_1'\alpha_1 + a_2'\alpha_2 + \cdots + a_n'\alpha_n \\
\mu_2 &= a_1''\alpha_1 + a_2''\alpha_2 + \cdots + a_n''\alpha_n \\
&\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot \\
\mu_n &= a_1^{(n)}\alpha_1 + a_2^{(n)}\alpha_2 + \cdots + a_n^{(n)}\alpha_n,
\end{aligned}$$

wo die Coefficienten a ganze rationale Zahlen bedeuten, so ist

$$(\mathfrak{a}, \mathfrak{m}) = \pm \sum \pm\, a_1' a_2'' \cdots a_n^{(n)}.$$

Von besonderer Wichtigkeit ist noch der folgende Satz: besteht eine Basis eines endlichen Moduls $\mathfrak{a}$ aus m Zahlen $\alpha_1', \alpha_2' \cdots \alpha_m'$, von denen aber nur n von einander unabhängig sind, so giebt es immer eine aus n unabhängigen Zahlen $\alpha_1, \alpha_2 \cdots \alpha_n$ bestehende Basis desselben Moduls $\mathfrak{a}$.

5⁰. Durchläuft α alle Zahlen eines Moduls $\mathfrak{a}$, ebenso β alle Zahlen eines Moduls $\mathfrak{b}$, so bilden die Producte $\alpha\beta$ und alle Summen solcher Producte einen Modul, der das *Product* aus den *Factoren* $\mathfrak{a}$, $\mathfrak{b}$ heissen und mit $\mathfrak{a}\mathfrak{b}$ bezeichnet werden soll, aber keineswegs durch $\mathfrak{a}$ oder $\mathfrak{b}$ theilbar zu sein braucht. Offenbar ist $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$ und $(\mathfrak{a}\mathfrak{b})\mathfrak{c} = \mathfrak{a}(\mathfrak{b}\mathfrak{c}) = \mathfrak{a}\mathfrak{b}\mathfrak{c}$; die Bedeutung einer *Potenz* $\mathfrak{a}^r$ ist selbstverständlich. Aus $\mathfrak{a}' > \mathfrak{a}$ und $\mathfrak{b}' > \mathfrak{b}$ folgt $\mathfrak{a}'\mathfrak{b}' > \mathfrak{a}\mathfrak{b}$; ferner ist

$$\begin{aligned}
(\mathfrak{a}+\mathfrak{b})\mathfrak{c} &= \mathfrak{a}\mathfrak{c} + \mathfrak{b}\mathfrak{c}; \\
(\mathfrak{a}-\mathfrak{b})\mathfrak{c} &> \mathfrak{a}\mathfrak{c} - \mathfrak{b}\mathfrak{c}; \\
(\mathfrak{a}+\mathfrak{b})(\mathfrak{a}-\mathfrak{b}) &> \mathfrak{a}\mathfrak{b};
\end{aligned}$$

ist ferner $[1] > \mathfrak{o}$, so ist $\mathfrak{a} > \mathfrak{o}\mathfrak{a}$, weil $\mathfrak{a}[1] = \mathfrak{a}$ ist. Ist $\mathfrak{b}$ ein eingliedriger Modul $[\mu]$, so besteht das Product $\mathfrak{a}\mathfrak{b}$ aus den Producten $\alpha\mu$, wo α alle Zahlen des Moduls $\mathfrak{a}$ durchläuft; ein solches Product $\mathfrak{a}[\mu]$ soll bequemer durch $\mathfrak{a}\mu = \mu\mathfrak{a}$ bezeichnet werden; dann ist $(\mathfrak{a}\mu)\nu = \mathfrak{a}(\mu\nu)$, und aus $\mathfrak{a}\mu = \mathfrak{a}'\mu$ folgt immer $\mathfrak{a} = \mathfrak{a}'$, wenn μ von 0 verschieden ist.

6⁰. Ist $\mathfrak{a}$ ein beliebiger Modul, so bildet das System $\mathfrak{o}$ aller derjenigen Zahlen ω, für welche das Product $\mathfrak{a}\omega > \mathfrak{a}$ wird, einen Modul, welcher die *Ordnung des Moduls* $\mathfrak{a}$ heissen soll und offenbar stets ein Theiler des Moduls $[1]$ ist; hieraus folgt unmittelbar, dass $\mathfrak{a}\mathfrak{o} = \mathfrak{a}$, und $\mathfrak{o}^2 = \mathfrak{o}$ ist. Umgekehrt ist jeder Modul

$\mathfrak{o}$, der ein Theiler von [1] und von $\mathfrak{o}^2$ ist, eine Ordnung, nämlich diejenige des Moduls $\mathfrak{o}$ selbst. Der Begriff einer Ordnung bildet eigentlich nur einen speciellen Fall des Begriffes des *Quotienten* $\mathfrak{a} : \mathfrak{b}$ von zwei beliebigen Moduln $\mathfrak{a}$, $\mathfrak{b}$, worunter der grösste gemeinschaftliche Theiler aller derjenigen Moduln $\mathfrak{c}$ zu verstehen ist, für welche das Product $\mathfrak{b}\mathfrak{c}$ durch $\mathfrak{a}$ theilbar wird; die Ordnung $\mathfrak{o}$ eines Moduls $\mathfrak{a}$ ist nämlich identisch mit dem Quotienten $\mathfrak{a} : \mathfrak{a}$, und die charakteristische Eigenschaft einer jeden Ordnung $\mathfrak{o}$ wird durch die Gleichung $\mathfrak{o} : \mathfrak{o} = \mathfrak{o}$ ausgedrückt. Doch wird von dem Begriffe des Quotienten in dieser Abhandlung kein Gebrauch gemacht werden.

§. 3.

Ordnungen in einem endlichen Körper.

Nach diesen allgemeinen Vorbereitungen kehren wir definitiv zu den Zahlen eines endlichen Körpers Ω vom Grade n zurück, und beschränken zunächst den Begriff des Moduls in der Weise, dass unter einem Modul $\mathfrak{a}$ stets ein endlicher Modul $[\alpha_1, \alpha_2 \cdots \alpha_n]$ verstanden wird, dessen Basiszahlen $\alpha_1, \alpha_2 \cdots \alpha_n$ zugleich eine Basis des Körpers Ω bilden (§. 1) und folglich von einander unabhängig sind (§. 2, 4⁰). Da hiernach jede Zahl des Körpers Ω durch Multiplication mit einer rationalen, von 0 verschiedenen Zahl in eine Zahl des Moduls $\mathfrak{a}$ verwandelt werden kann, so ergiebt sich aus den vorhergehenden allgemeinen Sätzen sehr leicht, dass das kleinste gemeinschaftliche Vielfache, der grösste gemeinschaftliche Theiler, und ebenso das Product (und auch der Quotient) von je zwei solchen Moduln $\mathfrak{a}$, $\mathfrak{b}$ stets wieder ein solcher Modul, und dass $(\mathfrak{a}, \mathfrak{b})$ stets von 0 verschieden ist. Versteht man ferner wie früher, und wie es auch in der Folge stets geschehen soll, unter $\mathfrak{o}$ das Gebiet *aller* ganzen Zahlen des Körpers Ω, so kommt die Definition eines Ideals $\mathfrak{m}$ (§. 1, 1⁰) darauf hinaus, dass $\mathfrak{m}$ ein durch $\mathfrak{o}$ theilbarer Modul ist (I), welcher der Bedingung $\mathfrak{o}\mathfrak{m} = \mathfrak{m}$ genügt (II); die dortigen Sätze 5⁰, 6⁰, 9⁰ enthalten nur noch die Behauptung, dass das kleinste gemeinschaftliche Vielfache, der grösste gemeinschaftliche Theiler und das Product von zwei beliebigen Idealen wieder Ideale sind; die Norm eines Ideals $\mathfrak{m}$ ist $= (\mathfrak{o}, \mathfrak{m})$.

Für die in Aussicht genommene Erweiterung des Ideal-Begriffs ist nun vor Allem die Constitution der *Ordnung* $\mathfrak{o}'$ eines beliebigen Moduls $\mathfrak{a} = [\alpha_1, \alpha_2 \cdots \alpha_n]$ von Wichtigkeit (§. 2, 6⁰). Damit eine Zahl ω' der Ordnung $\mathfrak{o}'$ des Moduls $\mathfrak{a}$ angehöre, ist offenbar erforderlich und hinreichend, dass die n Producte $\omega'\alpha_1$, $\omega'\alpha_2 \cdots \omega'\alpha_n$ in $\mathfrak{a}$ enthalten sind, dass also

$$\begin{aligned}
\omega'\alpha_1 &= x_1'\alpha_1 + x_2'\alpha_2 + \cdots + x_n'\alpha_n \\
\omega'\alpha_2 &= x_1''\alpha_1 + x_2''\alpha_2 + \cdots + x_n''\alpha_n \\
&\cdots\cdots\cdots\cdots \\
\omega'\alpha_n &= x_1^{(n)}\alpha_1 + x_2^{(n)}\alpha_2 + \cdots + x_n^{(n)}\alpha_n
\end{aligned}$$

ist, wo die n^2 Coefficienten x sämmtlich *ganze* rationale Zahlen bedeuten. Aus jeder einzelnen dieser Gleichungen folgt zunächst, dass ω' eine Zahl des Körpers Ω ist, und wenn man die n Zahlen $\alpha_1, \alpha_2 \cdots \alpha_n$ eliminirt, so erhält man

$$\begin{vmatrix}
x_1' - \omega', & x_2' & \cdots & x_n' \\
x_1'', & x_2'' - \omega' & \cdots & x_n'' \\
\cdots & \cdots & \cdots & \cdots \\
x_1^{(n)}, & x_2^{(n)} & \cdots & x_n^{(n)} - \omega'
\end{vmatrix} = 0,$$

d. h. ω' ist eine ganze algebraische Zahl, also in dem Gebiete $\mathfrak{o}$ enthalten; mithin ist $\mathfrak{o}'$ ein *Vielfaches von* $\mathfrak{o}$. Versteht man jetzt für einen Augenblick unter ω' eine *beliebige* Zahl des Körpers Ω, so gehören auch die n Producte $\omega'\alpha_1, \omega'\alpha_2 \cdots \omega'\alpha_n$ dem Körper Ω an, und folglich werden, da $\alpha_1, \alpha_2 \cdots \alpha_n$ eine Basis des Körpers Ω bilden, wieder n Gleichungen von der obigen Form Statt finden, in welchen aber die n^2 rationalen Coefficienten x nicht mehr nothwendig ganze Zahlen sind; es wird dann immer eine von 0 verschiedene, rationale Zahl m von der Art geben, dass die sämmtlichen n^2 Producte *mx ganze* Zahlen werden, und folglich wird das Product $m\omega'$ eine Zahl der Ordnung $\mathfrak{o}'$ sein; jede Zahl des Körpers Ω, also auch jede Zahl des Gebietes $\mathfrak{o}$ kann daher durch Multiplication mit einer von 0 verschiedenen rationalen Zahl in eine Zahl der Ordnung $\mathfrak{o}'$ verwandelt werden, und da das Gebiet $\mathfrak{o} = [\omega_1, \omega_2 \cdots \omega_n]$ ein Theiler von $\mathfrak{o}'$ ist, so ist (nach §. 2, 3⁰) $\mathfrak{o}'$ ein endlicher Modul $[\omega_1', \omega_2' \cdots \omega_n']$, dessen Basiszahlen mit denen von $\mathfrak{o}$ durch n Gleichungen von der Form

$$\omega_1' = k_1' \omega_1 + k_2' \omega_2 + \cdots + k_n' \omega_n$$
$$\omega_2' = k_1'' \omega_1 + k_2'' \omega_2 + \cdots + k_n'' \omega_n$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$\omega_n' = k_1^{(n)} \omega_1 + k_2^{(n)} \omega_2 + \cdots + k_n^{(n)} \omega_n$$

verbunden sind, deren Coefficienten ganze rationale Zahlen sind und eine von 0 verschiedene, positive Determinante

$$\sum \pm k_1' k_2'' \ldots k_n^{(n)} = (\mathfrak{o}, \mathfrak{o}') = k$$

besitzen. Die charakteristischen Eigenschaften einer solchen Ordnung $\mathfrak{o}'$ sind daher (§. 2, 6⁰) die folgenden:

1⁰. $\mathfrak{o}'$ ist ein durch $\mathfrak{o}$ theilbarer Modul im obigen beschränkten Sinne des Wortes; alle in $\mathfrak{o}'$ enthaltenen Zahlen sind ganze Zahlen des Körpers Ω.

2⁰. $\mathfrak{o}'$ ist ein Theiler von [1], d. h. alle ganzen rationalen Zahlen sind in $\mathfrak{o}'$ enthalten.

3⁰. $\mathfrak{o}'$ ist ein Theiler von $\mathfrak{o}'^2$, d. h. jedes Product von zwei in $\mathfrak{o}'$ enthaltenen Zahlen gehört ebenfalls dem System $\mathfrak{o}'$ an. Aus 2⁰ folgt dann $\mathfrak{o}'^2 = \mathfrak{o}'$.

Aus den obigen Gleichungen folgt nun durch Umkehrung, dass die n Producte $k\omega_1, k\omega_2 \cdots k\omega_n$ der Ordnung $\mathfrak{o}'$ angehören, und folglich ist das Hauptideal $\mathfrak{o}k$ theilbar durch $\mathfrak{o}'$. Da ferner der grösste gemeinschaftliche Theiler von je zwei durch $\mathfrak{o}'$ theilbaren Idealen selbst wieder ein durch $\mathfrak{o}'$ theilbares Ideal ist, so giebt es unter diesen, durch $\mathfrak{o}'$ theilbaren Idealen ein einziges, völlig bestimmtes Ideal $\mathfrak{k}$ von kleinster Norm, und die genannten Ideale sind (nach §. 1, 10⁰) identisch mit den sämmtlichen Producten $\mathfrak{a}\mathfrak{k}$, wo $\mathfrak{a}$ alle Ideale durchläuft. Dieses Ideal $\mathfrak{k}$ soll der *Führer der Ordnung* $\mathfrak{o}'$ heissen. Da das Hauptideal $\mathfrak{o}k$ durch $\mathfrak{o}'$ und folglich auch durch $\mathfrak{k}$ theilbar ist, so ist k^n als Norm von $\mathfrak{o}k$ theilbar durch

$$N(\mathfrak{k}) = (\mathfrak{o}, \mathfrak{k}) = (\mathfrak{o}, \mathfrak{o}')(\mathfrak{o}', \mathfrak{k}) = k(\mathfrak{o}', \mathfrak{k}).$$

Ist der Führer $\mathfrak{k}$ der Ordnung $\mathfrak{o}'$ und für jede der $(\mathfrak{o}', \mathfrak{k})$ Zahlclassen, aus denen $\mathfrak{o}'$ besteht, ein Repräsentant gegeben, so ist $\mathfrak{o}'$ vollständig definirt. Nicht jedes Ideal $\mathfrak{k}$ kann der Führer einer Ordnung sein, sondern hierzu ist eine gewisse Bedingung erforderlich, deren Auffindung keine grossen Schwierigkeiten darbietet; doch würde die Ableitung derselben sowie ein näheres Eingehen auf die Constitution der Ordnungen überhaupt, uns hier zu weit führen. Das Gebiet $\mathfrak{o}$ ist offenbar selbst eine Ordnung und auch zugleich der Führer derselben.

§. 4.

Ideale der Ordnung $\mathfrak{o}'$.

Es sei nun $\mathfrak{o}'$ eine bestimmte Ordnung im Körper Ω, und $\mathfrak{f}$ der Führer derselben, so wollen wir ein System $\mathfrak{a}'$ von unendlich vielen Zahlen ein *Ideal der Ordnung* $\mathfrak{o}'$ oder kürzer ein *Ideal in* $\mathfrak{o}'$ nennen, wenn es die folgenden drei Bedingungen erfüllt:

I. Die Summen und Differenzen von je zwei in $\mathfrak{a}'$ enthaltenen Zahlen gehören ebenfalls dem System $\mathfrak{a}'$ an, d. h. $\mathfrak{a}'$ ist ein Modul im allgemeinsten Sinne des Wortes.

II. Jedes Product aus einer Zahl des Systems $\mathfrak{a}'$ und aus einer Zahl der Ordnung $\mathfrak{o}'$ ist eine Zahl des Systems $\mathfrak{a}'$; d. h. $\mathfrak{o}'\mathfrak{a}'$ ist theilbar durch $\mathfrak{a}'$ und folglich auch $= \mathfrak{a}'$, weil $\mathfrak{o}'$ ein Theiler von $[1]$ ist.

III. Der grösste gemeinschaftliche Theiler $\mathfrak{a}' + \mathfrak{f}$ von $\mathfrak{a}'$ und $\mathfrak{f}$ ist $= \mathfrak{o}'$.

Für den Fall, dass die Ordnung $\mathfrak{o}'$ identisch mit $\mathfrak{o}$ ist, geht diese Definition eines Ideals $\mathfrak{a}'$ in $\mathfrak{o}'$ vollständig in die frühere Definition (§. 1, 1^0) eines Ideals über, da die dritte Bedingung nur darauf hinauskommt, dass $\mathfrak{a}'$ durch $\mathfrak{o}$ theilbar ist. Wir werden daher diese Ideale künftig, wenn Missverständnisse zu befürchten sind, *Ideale in* $\mathfrak{o}$ zu nennen haben. Im Folgenden nehmen wir immer an, dass $\mathfrak{o}'$ von $\mathfrak{o}$ verschieden ist.

Ist nun α' eine beliebige, aber von 0 verschiedene Zahl in $\mathfrak{a}'$, und bilden die n Zahlen $\omega_1', \omega_2' \cdots \omega_n'$ eine Basis der Ordnung $\mathfrak{o}'$, so sind die n Producte $\alpha'\omega_1', \alpha'\omega_2' \cdots \alpha'\omega_n'$, welche (zufolge II) in $\mathfrak{a}'$ enthalten sind, von einander unabhängig und bilden folglich eine Basis des Körpers Ω; mithin kann jede Zahl des Körpers durch Multiplication mit einer rationalen, von 0 verschiedenen Zahl in eine Zahl des Ideals $\mathfrak{a}'$ verwandelt werden, woraus wieder leicht folgt, dass $\mathfrak{a}'$ ein endlicher Modul $[\alpha_1', \alpha_2' \cdots \alpha_n']$, also ein Modul in dem Sinne des §. 3 ist. Die Basiszahlen haben die Form

$$\begin{aligned}
\alpha_1' &= a_1'\omega_1' + a_2'\omega_2' + \cdots + a_n'\omega_n' \\
\alpha_2' &= a_1''\omega_1' + a_2''\omega_2' + \cdots + a_n''\omega_n' \\
&\cdots\cdots\cdots\cdots\cdots \\
\alpha_n' &= a_1^{(n)}\omega_1' + a_2^{(n)}\omega_2' + \cdots + a_n^{(n)}\omega_n',
\end{aligned}$$

wo die Coefficienten ganze rationale Zahlen sind, deren Determinante

$$\sum \pm a_1' a_2'' \cdots a_n^{(n)} = (\mathfrak{o}', \mathfrak{a}')$$

die *Norm* des Ideals $\mathfrak{a}'$ heissen und mit $N'(\mathfrak{a}')$ bezeichnet werden soll.

Es ergiebt sich ferner leicht, dass $\mathfrak{o}'$ auch die Ordnung des Ideals $\mathfrak{a}'$ ist; in der That besteht die letztere, die wir mit $\mathfrak{o}_1$ bezeichnen wollen, zufolge ihrer Definition (§. 2, 6⁰) aus *allen* Zahlen ω_1, für welche $\mathfrak{a}'\omega_1 > \mathfrak{a}'$ wird, und da (nach II) $\mathfrak{a}'\mathfrak{o}' = \mathfrak{a}'$ ist, so ist jedenfalls $\mathfrak{o}' > \mathfrak{o}_1$, und es braucht nur noch bewiesen zu werden, dass umgekehrt auch $\mathfrak{o}_1 > \mathfrak{o}'$ ist. Da nun $\mathfrak{a}'$ ein endlicher Modul des Körpers, und folglich (nach §. 3, 1⁰ und 2⁰) $[1] > \mathfrak{o}_1 > \mathfrak{o}$ ist, so ergiebt sich $\mathfrak{k}[1] > \mathfrak{k}\mathfrak{o}_1 > \mathfrak{k}\mathfrak{o}$, mithin $\mathfrak{k}\mathfrak{o}_1 = \mathfrak{k}$, weil $\mathfrak{k}[1] = \mathfrak{k}\mathfrak{o} = \mathfrak{k}$ ist; da ausserdem (nach §. 2, 6⁰) $\mathfrak{a}'\mathfrak{o}_1 = \mathfrak{a}'$, und (nach III) $\mathfrak{o}' = \mathfrak{k} + \mathfrak{a}'$ ist, so folgt $\mathfrak{o}'\mathfrak{o}_1 = \mathfrak{k}\mathfrak{o}_1 + \mathfrak{a}'\mathfrak{o}_1 = \mathfrak{k} + \mathfrak{a}'$, also $\mathfrak{o}'\mathfrak{o}_1 = \mathfrak{o}'$; nun ist aber $[1] > \mathfrak{o}'$, also auch $[1]\mathfrak{o}_1 > \mathfrak{o}'\mathfrak{o}_1$, d. h. $\mathfrak{o}_1 > \mathfrak{o}'$, w. z. b. w.

Sind ferner $\mathfrak{a}', \mathfrak{b}'$ zwei beliebige Ideale in $\mathfrak{o}'$, so überzeugt man sich leicht, dass $\mathfrak{a}' - \mathfrak{b}'$, $\mathfrak{a}' + \mathfrak{b}'$, $\mathfrak{a}'\mathfrak{b}'$ ebenfalls Ideale in $\mathfrak{o}'$ sind, und dass $\mathfrak{a}'\mathfrak{b}'$ sowohl durch $\mathfrak{a}'$ als durch $\mathfrak{b}'$ theilbar ist. Der Kürze wegen beschränke ich mich auf die Betrachtung des Productes. Da $\mathfrak{o}'\mathfrak{a}' = \mathfrak{a}'$, so ergiebt sich $\mathfrak{o}'(\mathfrak{a}'\mathfrak{b}') = (\mathfrak{o}'\mathfrak{a}')\mathfrak{b}' = \mathfrak{a}'\mathfrak{b}'$, also besitzt $\mathfrak{a}'\mathfrak{b}'$ die Eigenschaft II. Da ferner $\mathfrak{b}' > \mathfrak{o}'$, und $\mathfrak{o}'\mathfrak{a}' = \mathfrak{a}'$ ist, so folgt $\mathfrak{a}'\mathfrak{b}' > \mathfrak{a}'$; ebenso ist $\mathfrak{a}'\mathfrak{b}'$ durch $\mathfrak{b}'$ theilbar. Da endlich $\mathfrak{o}' = \mathfrak{a}' + \mathfrak{k}$ ist, so folgt $\mathfrak{b}' = \mathfrak{o}'\mathfrak{b}' = \mathfrak{a}'\mathfrak{b}' + \mathfrak{k}\mathfrak{b}'$, also $\mathfrak{o}' = \mathfrak{b}' + \mathfrak{k} = \mathfrak{a}'\mathfrak{b}' + \mathfrak{k}\mathfrak{b}' + \mathfrak{k}$; da nun $\mathfrak{k} = \mathfrak{k}\mathfrak{o}$, und $\mathfrak{b}' > \mathfrak{o}$ ist, so folgt $\mathfrak{k}\mathfrak{b}' + \mathfrak{k} = \mathfrak{k}(\mathfrak{b}' + \mathfrak{o}) = \mathfrak{k}\mathfrak{o} = \mathfrak{k}$, also $\mathfrak{o}' = \mathfrak{a}'\mathfrak{b}' + \mathfrak{k}$, womit auch die Eigenschaft III für $\mathfrak{a}'\mathfrak{b}'$ dargethan ist.

§. 5.

Correspondenz zwischen den Idealen in $\mathfrak{o}'$ und $\mathfrak{o}$.

Man könnte nun eine Theorie der Ideale in $\mathfrak{o}'$ aufstellen, welche sowohl in den Sätzen wie in ihren Beweisen eine vollständige Analogie mit der früheren Theorie der Ideale in $\mathfrak{o}$ darbieten würde. Allein es ist viel bequemer, die neue Theorie auf die alte zurückzuführen. Dies geschieht durch die folgenden Sätze.

1⁰. *Ist $\mathfrak{a}'$ ein Ideal in $\mathfrak{o}'$, so ist $\mathfrak{o}\mathfrak{a}'$ ein Ideal in $\mathfrak{o}$, und zwar relatives Primideal zu $\mathfrak{k}$; zugleich ist $\mathfrak{a}'$ das kleinste gemeinschaftliche Vielfache, $\mathfrak{o}$ der grösste gemeinschaft-*

liche Theiler von $\mathfrak{o}'$ *und* $\mathfrak{o}\mathfrak{a}'$, *und folglich* $N'(\mathfrak{a}') = N(\mathfrak{o}\mathfrak{a}')$. *Ist ferner* $\mathfrak{b}'$ *ebenfalls ein Ideal in* $\mathfrak{o}'$, *und* $\mathfrak{o}\mathfrak{a}' = \mathfrak{o}\mathfrak{b}'$, *so ist* $\mathfrak{a}' = \mathfrak{b}'$.

Beweis. Der Modul $\mathfrak{o}\mathfrak{a}'$ genügt der Bedingung $\mathfrak{o}(\mathfrak{o}\mathfrak{a}') = \mathfrak{o}\mathfrak{a}'$, weil $\mathfrak{o}^2 = \mathfrak{o}$ ist, und er ist theilbar durch $\mathfrak{o}\mathfrak{o}' = \mathfrak{o}$, weil $\mathfrak{a}' > \mathfrak{o}'$ und $[1] > \mathfrak{o}' > \mathfrak{o}$ ist; also ist $\mathfrak{o}\mathfrak{a}'$ ein Ideal in $\mathfrak{o}$. Aus $\mathfrak{o}' = \mathfrak{a}' + \mathfrak{f}$ folgt durch Multiplication mit $\mathfrak{o}$ ferner $\mathfrak{o} = \mathfrak{o}\mathfrak{a}' + \mathfrak{f}$, also sind $\mathfrak{o}\mathfrak{a}'$ und $\mathfrak{f}$ relative Primideale. Hieraus ergiebt sich ferner (entweder nach der bekannten Theorie der Ideale in $\mathfrak{o}$, oder auch unmittelbar), dass ihr kleinstes gemeinschaftliches Vielfaches $\mathfrak{f} - \mathfrak{o}\mathfrak{a}' = \mathfrak{f}\mathfrak{o}\mathfrak{a}' = \mathfrak{f}\mathfrak{a}'$ ist. Wendet man nun den allgemeinen Satz (§. 2, 1⁰)

$$(\mathfrak{a}+\mathfrak{b}) - (\mathfrak{a}+\mathfrak{c}) = \mathfrak{a} + (\mathfrak{b}-(\mathfrak{a}+\mathfrak{c}))$$

auf den Fall $\mathfrak{a} = \mathfrak{a}'$, $\mathfrak{b} = \mathfrak{f}$, $\mathfrak{c} = \mathfrak{o}\mathfrak{a}'$ an, so ergiebt sich, weil $\mathfrak{a}' + \mathfrak{o}\mathfrak{a}' = (\mathfrak{o}'+\mathfrak{o})\mathfrak{a}' = \mathfrak{o}\mathfrak{a}'$ ist,

$$\begin{aligned} \mathfrak{o}' - \mathfrak{o}\mathfrak{a}' &= \mathfrak{a}' + (\mathfrak{f}-\mathfrak{o}\mathfrak{a}') = \mathfrak{a}' + \mathfrak{f}\mathfrak{a}' \\ &= \mathfrak{a}'(\mathfrak{o}'+\mathfrak{f}) = \mathfrak{a}'\mathfrak{o}' = \mathfrak{a}'. \end{aligned}$$

Ferner ist

$$\mathfrak{o}' + \mathfrak{o}\mathfrak{a}' = \mathfrak{f} + \mathfrak{a}' + \mathfrak{o}\mathfrak{a}' = \mathfrak{f} + \mathfrak{o}\mathfrak{a}' = \mathfrak{o}.$$

Hieraus ergiebt sich (nach §. 2, 2⁰)

$$(\mathfrak{o}', \mathfrak{o}\mathfrak{a}') = (\mathfrak{o}', \mathfrak{a}') = (\mathfrak{o}, \mathfrak{o}\mathfrak{a}'),$$

also $N'(\mathfrak{a}') = N(\mathfrak{o}\mathfrak{a}')$. Aus $\mathfrak{o}\mathfrak{a}' = \mathfrak{o}\mathfrak{b}'$ folgt endlich, weil $\mathfrak{a}' = \mathfrak{o}' - \mathfrak{o}\mathfrak{a}'$ und $\mathfrak{b}' = \mathfrak{o}' - \mathfrak{o}\mathfrak{b}'$ ist, auch $\mathfrak{a}' = \mathfrak{b}'$, w. z. b. w.

2⁰. *Ist* $\mathfrak{a}$ *ein Ideal in* $\mathfrak{o}$, *und zwar relatives Primideal zu* $\mathfrak{f}$, *so ist das kleinste gemeinschaftliche Vielfache* $\mathfrak{a}'$ *von* $\mathfrak{o}'$, $\mathfrak{a}$ *ein Ideal in* $\mathfrak{o}'$, *und zugleich ist* $\mathfrak{o}\mathfrak{a}' = \mathfrak{a}$.

Beweis. Zunächst ist $\mathfrak{o}'\mathfrak{a}' > \mathfrak{o}\mathfrak{a} = \mathfrak{a}$, weil $\mathfrak{o}' > \mathfrak{o}$, $\mathfrak{a}' > \mathfrak{a}$ ist; ausserdem ist $\mathfrak{o}'\mathfrak{a}' > \mathfrak{o}'$, weil $\mathfrak{a}' > \mathfrak{o}'$ und $\mathfrak{o}'\mathfrak{o}' = \mathfrak{o}'$ ist; mithin ist $\mathfrak{o}'\mathfrak{a}'$ ein gemeinschaftliches Vielfaches von $\mathfrak{o}'$, $\mathfrak{a}$ und folglich auch theilbar durch $\mathfrak{a}'$, d. h. $\mathfrak{a}'$ genügt der Bedingung II. Nach einem für drei beliebige Moduln $\mathfrak{a}$, $\mathfrak{f}$, $\mathfrak{o}'$ geltenden Satze (§. 2, 1⁰) ist ferner

$$(\mathfrak{o}'-\mathfrak{a}) + (\mathfrak{o}'-\mathfrak{f}) = \mathfrak{o}' - (\mathfrak{a}+(\mathfrak{o}'-\mathfrak{f})),$$

und da in unserem Falle $\mathfrak{o}' - \mathfrak{a} = \mathfrak{a}'$, $\mathfrak{o}' - \mathfrak{f} = \mathfrak{f}$, $\mathfrak{a} + \mathfrak{f} = \mathfrak{o}$, $\mathfrak{o}' - \mathfrak{o} = \mathfrak{o}'$ ist, so ergiebt sich $\mathfrak{a}' + \mathfrak{f} = \mathfrak{o}'$, also genügt $\mathfrak{a}'$ auch der Bedingung III und ist folglich ein Ideal in $\mathfrak{o}'$. Hieraus folgt (nach dem Satze 1⁰), dass $\mathfrak{o}\mathfrak{a}'$ ein Ideal in $\mathfrak{o}$, und dass zugleich $\mathfrak{o} = \mathfrak{o}\mathfrak{a}' + \mathfrak{f}$, also auch $\mathfrak{a} = \mathfrak{o}\mathfrak{a}'\mathfrak{a} + \mathfrak{f}\mathfrak{a}$ ist; da nun $\mathfrak{a}$, $\mathfrak{f}$ Ideale in $\mathfrak{o}$ sind, so

ist $\mathfrak{f}\mathfrak{a} > \mathfrak{f} > \mathfrak{o}'$ und $\mathfrak{f}\mathfrak{a} > \mathfrak{a}$, also muss $\mathfrak{f}\mathfrak{a}$, als gemeinschaftliches Vielfaches von $\mathfrak{o}'$, $\mathfrak{a}$, durch $\mathfrak{a}'$ und folglich auch durch $\mathfrak{o}\mathfrak{a}'$ theilbar sein; da nun auch $\mathfrak{o}\mathfrak{a}'\mathfrak{a}$ durch $\mathfrak{o}\mathfrak{a}'$ theilbar, also $\mathfrak{o}\mathfrak{a}'$ ein gemeinschaftlicher Theiler von $\mathfrak{f}\mathfrak{a}$ und $\mathfrak{o}\mathfrak{a}'\mathfrak{a}$ ist, so folgt, dass $\mathfrak{a}$ als grösster gemeinschaftlicher Theiler von $\mathfrak{o}\mathfrak{a}'\mathfrak{a}$ und $\mathfrak{f}\mathfrak{a}$ gewiss durch $\mathfrak{o}\mathfrak{a}'$ theilbar ist; umgekehrt ist aber auch $\mathfrak{o}\mathfrak{a}' > \mathfrak{a}$, weil $\mathfrak{a}' > \mathfrak{a}$ und $\mathfrak{o}\mathfrak{a} = \mathfrak{a}$ ist; mithin ist $\mathfrak{o}\mathfrak{a}' = \mathfrak{a}$, w. z. b. w.

Durch diese beiden Sätze ist eine eindeutige, gegenseitige Correspondenz zwischen allen Idealen $\mathfrak{a}'$ in $\mathfrak{o}'$ und allen denjenigen Idealen $\mathfrak{a}$ in $\mathfrak{o}$ begründet, welche relative Primideale zum Führer $\mathfrak{f}$ der Ordnung $\mathfrak{o}'$ sind; die Correspondenz zwischen $\mathfrak{a}$ und $\mathfrak{a}'$ besteht darin, dass gleichzeitig $\mathfrak{a} = \mathfrak{o}\mathfrak{a}'$, und $\mathfrak{a}' = \mathfrak{o}' - \mathfrak{a}$ ist. Offenbar entsprechen sich auf diese Weise die beiden Ideale $\mathfrak{o}$ und $\mathfrak{o}'$.

Es ist schon oben (§. 4) bewiesen, dass jedes Product $\mathfrak{a}'\mathfrak{b}'$ aus zwei Idealen $\mathfrak{a}'$, $\mathfrak{b}'$ in $\mathfrak{o}'$ wieder ein Ideal $\mathfrak{c}'$ in $\mathfrak{o}'$ und zwar durch $\mathfrak{a}'$ und durch $\mathfrak{b}'$ theilbar ist; da nun $\mathfrak{o}^2 = \mathfrak{o}$ ist, so ist gleichzeitig $\mathfrak{o}\mathfrak{a}' \cdot \mathfrak{o}\mathfrak{b}' = \mathfrak{o}\mathfrak{a}'\mathfrak{b}' = \mathfrak{o}\mathfrak{c}'$, also (nach §. 1, 9⁰) $N(\mathfrak{o}\mathfrak{a}'\mathfrak{b}') = N(\mathfrak{o}\mathfrak{a}')N(\mathfrak{o}\mathfrak{b}')$ und folglich auch

$$N'(\mathfrak{a}'\mathfrak{b}') = N'(\mathfrak{a}')N'(\mathfrak{b}').$$

Umgekehrt: wenn $\mathfrak{a}'$, $\mathfrak{c}'$ Ideale in $\mathfrak{o}'$ sind, und wenn $\mathfrak{c}'$ durch $\mathfrak{a}'$ theilbar ist, so ist auch $\mathfrak{o}\mathfrak{c}' > \mathfrak{o}\mathfrak{a}'$, und folglich (§. 1, 10⁰) giebt es ein und nur ein Ideal $\mathfrak{b}$ in $\mathfrak{o}$, für welches $\mathfrak{o}\mathfrak{c}' = \mathfrak{o}\mathfrak{a}'\mathfrak{b}$ wird; da nun $\mathfrak{o}\mathfrak{c}'$, also auch $\mathfrak{b}$, relatives Primideal zu $\mathfrak{f}$ ist, so giebt es (nach 2⁰) ein und nur ein Ideal $\mathfrak{b}'$ in $\mathfrak{o}'$, für welches $\mathfrak{o}\mathfrak{b}' = \mathfrak{b}$ wird; es ist daher $\mathfrak{o}\mathfrak{c}' = \mathfrak{o}\mathfrak{a}' \cdot \mathfrak{o}\mathfrak{b}' = \mathfrak{o}(\mathfrak{a}'\mathfrak{b}')$, woraus (nach 1⁰) $\mathfrak{c}' = \mathfrak{a}'\mathfrak{b}'$ folgt; wäre nun zugleich $\mathfrak{c}' = \mathfrak{a}'\mathfrak{d}'$ und $\mathfrak{d}'$ ebenfalls ein Ideal in $\mathfrak{o}'$, so würde $\mathfrak{o}\mathfrak{c}' = \mathfrak{o}\mathfrak{a}' \cdot \mathfrak{o}\mathfrak{d}' = \mathfrak{o}\mathfrak{a}' \cdot \mathfrak{o}\mathfrak{b}'$, und hieraus (nach §. 1, 10⁰) $\mathfrak{o}\mathfrak{d}' = \mathfrak{o}\mathfrak{b}'$, also auch $\mathfrak{d}' = \mathfrak{b}'$ folgen. Hiermit ist folgender Satz bewiesen:

3⁰. *Ist das Ideal* $\mathfrak{c}'$ *in* $\mathfrak{o}'$ *theilbar durch das Ideal* $\mathfrak{a}'$ *in* $\mathfrak{o}'$, *so giebt es ein und nur ein Ideal* $\mathfrak{b}'$ *in* $\mathfrak{o}'$ *von der Art, dass* $\mathfrak{a}'\mathfrak{b}' = \mathfrak{c}'$ *wird; ausserdem ist immer* $N'(\mathfrak{a}'\mathfrak{b}') = N'(\mathfrak{a}')N'(\mathfrak{b}')$.

Aus allem Diesen ergiebt sich ohne Weiteres, dass die Gesetze der Theilbarkeit der Ideale in $\mathfrak{o}'$ und ihrer Multiplication gänzlich mit den Gesetzen der Theilbarkeit derjenigen Ideale in $\mathfrak{o}$, welche relative Primideale zu $\mathfrak{f}$ sind, übereinstimmen und durch die genannte Correspondenz aus den letzteren unmittelbar entnommen werden.

§. 6.

Hauptideale und Ideal-Classen in $\mathfrak{o}'$.

Zwei Moduln $\mathfrak{a}$, $\mathfrak{b}$ des Körpers Ω, d. h. endliche Moduln, deren Basen zugleich Basen des Körpers sind (§. 3), sollen *äquivalent* heissen, wenn es eine Zahl μ von der Beschaffenheit giebt, dass $\mathfrak{a}\mu = \mathfrak{b}$, und folglich, da μ nicht verschwinden kann, auch $\mathfrak{b}\mu^{-1} = \mathfrak{a}$ wird. Offenbar muss μ eine Zahl des Körpers Ω sein, und wir wollen dem vorstehenden Begriffe der *Aequivalenz* noch die Beschränkung hinzufügen, dass $\mathfrak{a}$, $\mathfrak{b}$ nur dann äquivalent heissen sollen, wenn eine Zahl μ von der genannten Beschaffenheit existirt, deren *Norm* zugleich *positiv* ist; wenn aber der Bedingung $\mathfrak{a}\mu = \mathfrak{b}$ nur durch solche Zahlen μ genügt werden kann, deren Normen *negativ* sind, so können $\mathfrak{a}$, $\mathfrak{b}$ *halb-äquivalent* genannt werden. Sind zwei Moduln $\mathfrak{b}$, $\mathfrak{c}$ mit einem dritten $\mathfrak{a}$ äquivalent, so sind $\mathfrak{b}$, $\mathfrak{c}$ offenbar auch mit einander äquivalent. Man kann daher die Moduln des Körpers Ω in *Modul-Classen* eintheilen, deren jede aus allen den Moduln besteht, welche mit einem bestimmten Modul, dem *Repräsentanten* der Classe, äquivalent sind. Alle Moduln einer Classe besitzen dieselbe Ordnung $\mathfrak{o}'$, welche die *Ordnung der Classe* heissen soll; denn wenn $\mathfrak{a}\mu = \mathfrak{b}$, und ω' irgend eine Zahl ist, für welche $\mathfrak{a}\omega' > \mathfrak{a}$ wird, so folgt durch Multiplication mit μ oder $[\mu]$, dass auch $\mathfrak{b}\omega' > \mathfrak{b}$ ist, und umgekehrt ergiebt sich hieraus wieder $\mathfrak{a}\omega' > \mathfrak{a}$. Durchläuft $\mathfrak{a}$ alle Moduln einer Classe A, ebenso $\mathfrak{b}$ alle Moduln einer Classe B, so gehören offenbar alle Producte $\mathfrak{a}\mathfrak{b}$ einer und derselben Classe an, welche die aus A, B *zusammengesetzte* Classe oder das *Product aus* A, B heissen und mit AB bezeichnet werden soll.

Wir beschränken uns aber hier auf die Betrachtung der *Ideale* und verstehen unter einer *Ideal-Classe* der Ordnung $\mathfrak{o}'$ den Inbegriff A' aller Ideale in $\mathfrak{o}'$, welche mit einem bestimmten Ideal $\mathfrak{a}'$ in $\mathfrak{o}'$ äquivalent sind. Jedes mit $\mathfrak{o}'$ selbst äquivalente Ideal soll ein *Hauptideal in* $\mathfrak{o}'$, und der Inbegriff aller dieser Hauptideale soll die *Hauptclasse in* $\mathfrak{o}'$ heissen und mit O' bezeichnet werden. Ein solches Hauptideal ist daher von der Form $\mathfrak{o}'\mu$, wo μ in $\mathfrak{o}'$ enthalten ist, weil $\mathfrak{o}'\mu$ durch $\mathfrak{o}'$ theilbar sein muss; ausserdem muss das zugehörige Ideal $\mathfrak{o}\mathfrak{o}'\mu = \mathfrak{o}\mu$ relatives Primideal zu $\mathfrak{f}$, d. h. μ muss relative Primzahl zu $\mathfrak{f}$ sein (D. §. 163, 7.). Umgekehrt, ist die in $\mathfrak{o}'$ enthaltene Zahl μ relative Primzahl zu $\mathfrak{f}$, und ist $N(\mu) > 0$, so ist $\mathfrak{o}'\mu$ offen-

bar ein Hauptideal in $\mathfrak{o}'$. Nun besteht folgender Satz, von welchem wichtige Anwendungen zu machen sind:

1°. *Ist* $\mathfrak{a}'$ *ein Ideal in* $\mathfrak{o}'$, *und* $\mathfrak{n}'$ *ein durch* $\mathfrak{o}'$ *theilbarer Modul, welcher der Bedingung* $\mathfrak{o}'\mathfrak{n}' = \mathfrak{n}'$ *genügt, so giebt es immer ein Ideal* $\mathfrak{b}'$ *in* $\mathfrak{o}'$ *von der Art, dass* $\mathfrak{a}'\mathfrak{b}'$ *ein Hauptideal in* $\mathfrak{o}'$, *und* $\mathfrak{b}' + \mathfrak{n}' = \mathfrak{o}'$ *wird.*

Beweis. Der Modul $\mathfrak{o}\mathfrak{n}'$ ist ein Ideal in $\mathfrak{o}$, weil er durch $\mathfrak{o}$ theilbar ist und der Bedingung $\mathfrak{o}(\mathfrak{o}\mathfrak{n}') = \mathfrak{o}\mathfrak{n}'$ genügt. Man zerlege nun $\mathfrak{o}\mathfrak{n}'$ in seine sämmtlichen Primideal-Factoren (§. 1, 12°) und bezeichne mit $\mathfrak{k}_1$ das Product aller derjenigen dieser Primideale, welche in $\mathfrak{k}$ aufgehen, mit $\mathfrak{n}_1$ das Product aller übrigen, so dass $\mathfrak{o}\mathfrak{n}' = \mathfrak{k}_1\mathfrak{n}_1$ wird. Nun giebt es (§. 1, 14° oder D. §. 163, 7.) immer ein Ideal $\mathfrak{m}_1$ in $\mathfrak{o}$ von der Art, dass $\mathfrak{o}\mathfrak{a}'\mathfrak{m}_1 = \mathfrak{a}'\mathfrak{m}_1 = \mathfrak{o}\alpha$, d. h. ein Hauptideal in $\mathfrak{o}$, und dass zugleich $\mathfrak{m}_1 + \mathfrak{n}_1 = \mathfrak{o}$, also $\mathfrak{o}\alpha + \mathfrak{a}'\mathfrak{n}_1 = \mathfrak{o}\mathfrak{a}'$ wird. Da ferner $\mathfrak{a}'$ ein Ideal in $\mathfrak{o}'$, also $\mathfrak{o}\mathfrak{a}'$ relatives Primideal zu $\mathfrak{k}$ ist, so sind auch $\mathfrak{o}\mathfrak{a}'\mathfrak{n}_1 = \mathfrak{a}'\mathfrak{n}_1$ und $\mathfrak{k}\mathfrak{k}_1$ relative Primideale, und folglich (§. 2, 2° oder D. §. 163, 7.) giebt es Zahlen μ, welche den beiden gleichzeitigen Congruenzen

$$\mu \equiv \alpha (\text{mod. } \mathfrak{a}'\mathfrak{n}_1), \; \mu \equiv 1 (\text{mod. } \mathfrak{k}\mathfrak{k}_1)$$

genügen; diese Zahlen μ bilden eine bestimmte Zahl-Classe in Bezug auf den Modul $\mathfrak{a}'\mathfrak{n}_1\mathfrak{k}\mathfrak{k}_1 = \mathfrak{k}\mathfrak{a}'\mathfrak{n}'$, und man kann, wie unten nachträglich bewiesen werden soll, die Zahl μ zugleich so wählen, dass $N(\mu) > 0$ wird. Aus der zweiten der beiden vorstehenden Congruenzen folgt nun, dass μ relative Primzahl zu $\mathfrak{k}\mathfrak{k}_1$ und folglich auch zu $\mathfrak{k}$ ist; da ferner $\mathfrak{k}\mathfrak{k}_1 > \mathfrak{k} > \mathfrak{o}'$, und da die Zahl 1 in der Ordnung $\mathfrak{o}'$ enthalten ist, so ist zufolge der zweiten Congruenz auch μ in $\mathfrak{o}'$ enthalten, und folglich ist $\mathfrak{o}'\mu$ ein Hauptideal in $\mathfrak{o}'$. Aus der ersten Congruenz folgt ferner mit Rücksicht auf $\mathfrak{o}\alpha + \mathfrak{a}'\mathfrak{n}_1 = \mathfrak{o}\mathfrak{a}'$, dass auch $\mathfrak{o}\mu + \mathfrak{a}'\mathfrak{n}_1 = \mathfrak{o}\mathfrak{a}'$, und folglich $\mathfrak{o}\mu = \mathfrak{o}\mathfrak{a}'\mathfrak{b} = \mathfrak{a}'\mathfrak{b}$ ist, wo $\mathfrak{b}$ ein Ideal in $\mathfrak{o}$, und zwar relatives Primideal zu $\mathfrak{n}_1$ ist. Da ferner $\mathfrak{o}\mu$, und folglich auch $\mathfrak{b}$ relatives Primideal zu $\mathfrak{k}\mathfrak{k}_1$ ist, so ist $\mathfrak{b}$ auch relatives Primideal zu $\mathfrak{k}\mathfrak{k}_1\mathfrak{n}_1 = \mathfrak{k}\mathfrak{n}'$, also $\mathfrak{b} + \mathfrak{k}\mathfrak{n}' = \mathfrak{o}$. Bedeutet ferner $\mathfrak{b}'$ das dem Ideale $\mathfrak{b}$ entsprechende Ideal in $\mathfrak{o}'$ (§. 5), so ist $\mathfrak{b} = \mathfrak{o}\mathfrak{b}'$, und aus $\mathfrak{o}\mu = \mathfrak{a}'\mathfrak{b}$, d. h. aus $\mathfrak{o}(\mathfrak{o}'\mu) = \mathfrak{o}(\mathfrak{a}'\mathfrak{b}')$ folgt $\mathfrak{o}'\mu = \mathfrak{a}'\mathfrak{b}'$. Nun ist $\mathfrak{k} > \mathfrak{o}'$ und nach Voraussetzung $\mathfrak{o}'\mathfrak{n}' = \mathfrak{n}'$, folglich $\mathfrak{k}\mathfrak{n}' > \mathfrak{n}'$, und da ebenfalls $\mathfrak{n}' > \mathfrak{o}'$ vorausgesetzt ist, so folgt $\mathfrak{k}\mathfrak{n}' > \mathfrak{o}'$, also $\mathfrak{o}' - \mathfrak{k}\mathfrak{n}' = \mathfrak{k}\mathfrak{n}'$; wendet man daher den allgemeinen Satz (§. 2, 1°)

$$(\mathfrak{a} - \mathfrak{b}) + (\mathfrak{a} - \mathfrak{c}) = \mathfrak{a} - (\mathfrak{b} + (\mathfrak{a} - \mathfrak{c}))$$

auf den Fall $\mathfrak{a} = \mathfrak{o}'$, $\mathfrak{c} = \mathfrak{f}\mathfrak{n}'$ an und berücksichtigt ausserdem, dass $\mathfrak{o}' - \mathfrak{b} = \mathfrak{b}'$, und $\mathfrak{b} + \mathfrak{f}\mathfrak{n}' = \mathfrak{o}$ ist, so folgt $\mathfrak{b}' + \mathfrak{f}\mathfrak{n}' = \mathfrak{o}' - \mathfrak{o} = \mathfrak{o}'$, woraus mit Rücksicht auf $\mathfrak{f}\mathfrak{n}' > \mathfrak{n}' > \mathfrak{o}'$ sich endlich auch $\mathfrak{b}' + \mathfrak{n}' = \mathfrak{o}'$ ergiebt, w. z. b. w.

Es ist nun noch der oben vorläufig übergangene Beweis nachzuholen, dass man μ so wählen kann, dass $N(\mu)$ *positiv* wird. Dies geschieht offenbar durch den Beweis des folgenden allgemeineren Satzes:

2⁰. *Ist* $\mathfrak{m}$ *ein Modul des Körpers* Ω, *und* μ_0 *eine bestimmte Zahl dieses Körpers, so giebt es unter den Zahlen* μ, *welche* $\equiv \mu_0$ (mod. $\mathfrak{m}$) *sind, unendlich viele, die eine positive Norm haben.*

Beweis. Dieser Satz ist selbstverständlich, sobald die sämmtlichen Wurzeln der Gleichung $f(\theta) = 0$, aus welcher der Körper Ω abgeleitet ist, imaginär, und folglich die n Factoren von $N(\mu) = \mu'\mu'' \cdots \mu^{(n)}$ aus $\frac{1}{2}n$ Paaren von zwei Zahlen $a + bi$, $a - bi$ bestehen; und wenn die Gleichung eine oder mehrere reelle Wurzeln hat, so braucht man offenbar nur die diesen Wurzeln entsprechenden Factoren von $N(\mu)$ zu betrachten, weil das Product der übrigen gewiss positiv ist. Da nun nach Voraussetzung die Basiszahlen des endlichen Moduls $\mathfrak{m}$ zugleich eine Basis des Körpers Ω bilden, so kann die dem Körper angehörende Zahl 1 durch Multiplication mit einer positiven rationalen Zahl m in eine Zahl m des Moduls $\mathfrak{m}$ verwandelt werden, und wenn h eine beliebige ganze rationale Zahl bedeutet, so wird $hm \equiv 0$ (mod. $\mathfrak{m}$), und folglich $\mu = \mu_0 + hm \equiv \mu_0$ (mod. $\mathfrak{m}$). Offenbar kann man nun die ganze rationale Zahl h positiv und so gross wählen, dass diejenigen Factoren

$$\mu' = \mu_0' + hm,\ \mu'' = \mu_0'' + hm \cdots \mu^{(n)} = \mu_0^{(n)} + hm,$$

welche den reellen Wurzeln der Gleichung $f(\theta) = 0$ entsprechen, sämmtlich positiv ausfallen, womit der Satz bewiesen ist.

§. 7.

Composition der Ideal-Classen.

Sind $\mathfrak{o}'$, $\mathfrak{o}''$ zwei beliebige Ordnungen des Körpers Ω, und $\mathfrak{f}'$, $\mathfrak{f}''$ ihre Führer, so ist offenbar ihr Product $\mathfrak{o}''' = \mathfrak{o}'\mathfrak{o}''$ ebenfalls eine Ordnung (§. 3), und da $\mathfrak{o}'''$ ein gemeinschaftlicher Theiler von $\mathfrak{o}'$, $\mathfrak{o}''$ ist, so muss der Führer $\mathfrak{f}'''$ der Ordnung $\mathfrak{o}'''$ auch ein gemeinschaftlicher Theiler von $\mathfrak{f}'$, $\mathfrak{f}''$ sein. Ist nun $\mathfrak{a}'$ ein beliebiges

Ideal in $\mathfrak{o}'$, ebenso $\mathfrak{b}''$ ein beliebiges Ideal in $\mathfrak{o}''$, so wird $\mathfrak{a}'\mathfrak{b}'' = \mathfrak{c}'''$ ein Ideal in $\mathfrak{o}'''$; denn aus $\mathfrak{o}'\mathfrak{a}' = \mathfrak{a}'$, $\mathfrak{o}''\mathfrak{b}'' = \mathfrak{b}''$ folgt $\mathfrak{o}'''\mathfrak{c}''' = \mathfrak{o}'\mathfrak{o}''\mathfrak{a}'\mathfrak{b}'' = \mathfrak{a}'\mathfrak{b}'' = \mathfrak{c}'''$; aus $\mathfrak{a}' + \mathfrak{k}' = \mathfrak{o}'$, $\mathfrak{b}'' + \mathfrak{k}'' = \mathfrak{o}''$ ergiebt sich ferner durch Multiplication

$$\mathfrak{a}'\mathfrak{b}'' + \mathfrak{a}'\mathfrak{k}'' + \mathfrak{k}'\mathfrak{b}'' + \mathfrak{k}'\mathfrak{k}'' = \mathfrak{o}'''$$

und hieraus, weil jedes der Ideale $\mathfrak{a}'\mathfrak{k}''$, $\mathfrak{k}'\mathfrak{b}''$, $\mathfrak{k}'\mathfrak{k}''$ durch $\mathfrak{k}'''$, und $\mathfrak{k}'''$ durch $\mathfrak{o}'''$ theilbar ist, $\mathfrak{a}'\mathfrak{b}'' + \mathfrak{k}''' = \mathfrak{o}'''$; also besitzt der Modul $\mathfrak{a}'\mathfrak{b}''$ die charakteristischen Eigenschaften eines Ideals in $\mathfrak{o}'''$ (§. 4), und da allgemein bewiesen ist, dass die Ordnung eines Ideals in $\mathfrak{o}'$ identisch mit $\mathfrak{o}'$ ist, so ergiebt sich, dass die Ordnung eines Productes von Idealen gleich dem Producte aus den Ordnungen der Factoren ist*).

Ist $\mathfrak{a}'$ ein Repräsentant der Ideal-Classe A' in $\mathfrak{o}'$, und $\mathfrak{b}''$ ein Repräsentant der Ideal-Classe B'' in $\mathfrak{o}''$, so ist jedes Product von zwei beliebigen Idealen in A', B'' von der Form $\mathfrak{a}'\mu \cdot \mathfrak{b}''\nu = \mathfrak{a}'\mathfrak{b}''(\mu\nu)$, also ein mit $\mathfrak{a}'\mathfrak{b}''$ äquivalentes Ideal; alle diese Producte gehören daher einer und derselben Ideal-Classe in $\mathfrak{o}'''$ an, welche (wie bei den Moduln) die aus A', B'' *zusammengesetzte* Classe oder das *Product* aus A', B'' heissen und mit $A'B''$ bezeichnet werden soll. Bedeuten A, B, C beliebige Ideal-Classen beliebiger Ordnungen, so ist offenbar $AB = BA$, $(AB)C = A(BC)$.

Von dieser allgemeinsten Composition der Ideal-Classen aller Ordnungen kehren wir zurück zu der Betrachtung der Ideal-Classen einer einzigen Ordnung $\mathfrak{o}'$; jedes Product von solchen Classen gehört derselben Ordnung $\mathfrak{o}'$ an, weil $\mathfrak{o}'^2 = \mathfrak{o}'$ ist. Da das Product $\mathfrak{o}'\mu \cdot \mathfrak{a}' = \mu\mathfrak{a}'$ aus einem Hauptideal $\mathfrak{o}'\mu$ und einem beliebigen Ideal $\mathfrak{a}'$ mit diesem letzteren äquivalent ist, so folgt $O'A' = A'$, wo A' eine beliebige Idealclasse in $\mathfrak{o}'$, und O' die Hauptclasse in $\mathfrak{o}'$ bedeutet. Da ferner, wenn $\mathfrak{a}'$ ein beliebiger Repräsentant der Ideal-Classe A' in $\mathfrak{o}'$ ist, immer ein solches Ideal $\mathfrak{b}'$ in $\mathfrak{o}'$ existirt, dass $\mathfrak{a}'\mathfrak{b}'$ ein Hauptideal in $\mathfrak{o}'$ wird, so giebt es eine Ideal-Classe B' in $\mathfrak{o}'$ von der Art, dass $A'B' = O'$ wird; und zwar giebt es nur eine einzige solche Classe B'; denn wenn C' ebenfalls eine Ideal-Classe in $\mathfrak{o}'$, und wenn $AC' = O'$ ist, so folgt $A'B'C' = O'B' = O'C' = B' = C'$. Diese Classe B' soll die zu A' gehörende *entgegengesetzte*, oder die *reciproke*, oder *inverse* Classe heissen und durch A'^{-1} bezeichnet werden; offenbar ist A' zugleich die inverse Classe von A'^{-1}. Sind

---

*) Wenn, wie es bei den quadratischen Körpern der Fall ist, jede Modul-Classe auch Ideale enthält, so gilt der obige Satz auch für Producte aus *Moduln;* aber schon bei cubischen Körpern giebt es Moduln, welche keinem Ideale äquivalent sind, und der obige Satz darf nicht mehr auf alle Producte von Moduln übertragen werden. Auf diese wichtige Frage werde ich bei einer anderen Gelegenheit zurückkommen.

nun A', B', C' beliebige Ideal-Classen derselben Ordnung $\mathfrak{o}'$, so folgt aus $A'B' = A'C'$ durch Multiplication mit A'^{-1} stets $B' = C'$ *). Sind ferner A', B' beliebige Ideal-Classen derselben Ordnung $\mathfrak{o}'$, so giebt es immer eine und nur eine Ideal-Classe $C' = A'^{-1}B'$ der Ordnung $\mathfrak{o}'$, welche der Bedingung $A'C' = B'$ genügt.

§. 8.

Correspondenz zwischen den Ideal-Classen in $\mathfrak{o}$ und $\mathfrak{o}'$.

Ist $\mathfrak{o}$ wieder die aus allen ganzen Zahlen des Körpers Ω bestehende Ordnung, O die Classe der Hauptideale in $\mathfrak{o}$, und $\mathfrak{o}'$ eine beliebige Ordnung, so wird durch jede bestimmte Ideal-Classe A' der Ordnung $\mathfrak{o}'$ eine bestimmte Ideal-Classe $OA' = A$ der Ordnung $\mathfrak{o}\mathfrak{o}' = \mathfrak{o}$ erzeugt, z. B. O selbst durch die Hauptclasse O' der Ordnung $\mathfrak{o}'$. Umgekehrt, ist A eine Ideal-Classe der Ordnung $\mathfrak{o}$, so giebt es in ihr immer einen Repräsentanten $\mathfrak{a}$, der relatives Primideal zum Führer $\mathfrak{k}$ der Ordnung $\mathfrak{o}'$ ist (denn nach §. 1, 14⁰ oder §. 6 oder D. §. 163, 7. kann jedes Ideal der inversen Classe A^{-1} durch Multiplication mit einem solchen Ideal $\mathfrak{a}$ in ein Hauptideal verwandelt werden, und dies muss folglich in A enthalten sein); dann ist $\mathfrak{a}' = \mathfrak{o}' - \mathfrak{a}$ das correspondirende Ideal in $\mathfrak{o}'$, und $\mathfrak{o}\mathfrak{a}' = \mathfrak{a}$ (§. 5, 2⁰), und wenn A' die Ideal-Classe in $\mathfrak{o}'$ ist, welcher $\mathfrak{a}'$ angehört, so ist $OA' = A$; also wird jede Ideal-Classe A der Ordnung $\mathfrak{o}$ durch *mindestens* eine Ideal-Classe A' der Ordnung $\mathfrak{o}'$ auf diese Weise erzeugt. Wir suchen nun zunächst *alle* Ideal-Classen B' der Ordnung $\mathfrak{o}'$, welche dieselbe Classe A hervorbringen, so dass $OB' = OA'$ wird; hieraus folgt aber $OB'A'^{-1} = OO'$, also, wenn

$$B'A'^{-1} = M', \quad B' = M'A'$$

gesetzt wird,

$$OM' = O.$$

Umgekehrt, wenn M' eine der vorstehenden Bedingung genügende Ideal-Classe der Ordnung $\mathfrak{o}'$, und wenn $B' = M'A'$ ist, so ist auch wirklich $OB' = OA'$.

Der Complex $\mathfrak{M}'$ aller dieser Ideal-Classen M', unter denen sich auch O' und jede inverse Classe M'^{-1} befindet, besitzt den Charakter einer *Gruppe*, insofern

---

*) Dieser Satz verliert, wie man leicht sieht, seine allgemeine Gültigkeit, wenn die Classen A', B', C' nicht derselben Ordnung angehören.

das Product von je zwei solchen Classen M' offenbar wieder demselben Complex $\mathfrak{M}'$ angehört. In den folgenden Paragraphen wird gezeigt werden, dass die Anzahl dieser Classen M' eine endliche ist; wir wollen dieselbe mit m bezeichnen und zunächst ihre Bedeutung für das Problem nachweisen, welches den Hauptgegenstand dieser Abhandlung bildet. Ist A' eine bestimmte Ideal-Classe in $\mathfrak{o}'$, und durchläuft M' alle m Classen der Gruppe $\mathfrak{M}'$, so bilden die sämmtlichen Producte $M'A'$ einen Complex von Classen der Ordnung $\mathfrak{o}'$, der mit $\mathfrak{M}'A'$ bezeichnet werden mag; da aus $M'_1A' = M'_2A'$ auch $M'_1 = M'_2$ folgt (§. 7), so besteht ein solcher Complex $\mathfrak{M}'A'$ aus m verschiedenen Classen. Enthalten ferner zwei solche Complexe $\mathfrak{M}'A'$, $\mathfrak{M}'B'$ eine und dieselbe Classe $M'_1A' = M'_2B'$, so ist $B' = M'^{-1}_2 M'_1 A' = M'_3 A'$, wo $M'_3 = M'^{-1}_2 M'_1$ ebenfalls in $\mathfrak{M}'$ enthalten ist, und hieraus folgt offenbar, dass die sämmtlichen m Classen des Complexes $\mathfrak{M}'B'$ mit denen von $\mathfrak{M}'A'$ vollständig übereinstimmen. Man kann daher alle Ideal-Classen der Ordnung $\mathfrak{o}'$ in lauter verschiedene solche Complexe von der Form $\mathfrak{M}'A'$, $\mathfrak{M}'B' \cdots$ eintheilen. Nun ist oben gezeigt, dass jede bestimmte Ideal-Classe A der Ordnung $\mathfrak{o}$ in der angegebenen Weise durch die sämmtlichen m Classen eines bestimmten solchen Complexes $\mathfrak{M}'A'$, und durch keine andere Classe der Ordnung $\mathfrak{o}'$ erzeugt wird, und dass umgekehrt alle m Classen eines solchen Complexes durch Multiplication mit O eine und nur eine Classe A der Ordnung $\mathfrak{o}$ erzeugen. Mithin ist die Anzahl aller dieser Complexe identisch mit der Anzahl h der verschiedenen Ideal-Classen der Ordnung $\mathfrak{o}$, deren Endlichkeit schon bewiesen ist (D. §. 164, 2⁰), und zugleich ergiebt sich, dass

$$h' = mh$$

die Anzahl aller verschiedenen Ideal-Classen der Ordnung $\mathfrak{o}'$ ist.

§. 9.

Bestimmung des Verhältnisses m der Classen-Anzahlen h' und h.

Es sei M' eine bestimmte Classe der Gruppe $\mathfrak{M}'$, und $\mathfrak{m}'$ ein bestimmter Repräsentant von M'. Da $OM' = O$ ist, so ist $\mathfrak{o}\mathfrak{m}'$ ein Hauptideal in $\mathfrak{o}$, also von der Form $\mathfrak{o}\mu$, wo μ eine ganze Zahl von positiver Norm und zwar relative Primzahl zu $\mathfrak{k}$ ist, wo $\mathfrak{k}$ wieder den Führer der Ordnung $\mathfrak{o}'$ bedeutet. Umgekehrt, ist μ eine solche Zahl, so ist $\mathfrak{o}\mu$ ein Hauptideal in $\mathfrak{o}$ und relatives Primideal zu $\mathfrak{k}$,

mithin giebt es (§. 5, 2^0) ein und nur ein Ideal $\mathfrak{m}'$ in $\mathfrak{o}'$, welches der Bedingung $\mathfrak{o}\mathfrak{m}' = \mathfrak{o}\mu$ genügt, und wenn M' die durch $\mathfrak{m}'$ repräsentirte Idealclasse in $\mathfrak{o}'$ bedeutet, so ist $OM' = O$; jeder bestimmten Zahl μ von der angegebenen Beschaffenheit entspricht daher auf diese Weise eine und nur eine Idealclasse M', welche der Gruppe $\mathfrak{M}'$ angehört. Auf diese Correspondenz bezieht sich der folgende Satz:

Sind μ, μ_1 ganze Zahlen von positiver Norm und relative Primzahlen zu $\mathfrak{k}$, so besteht die erforderliche und hinreichende Bedingung dafür, dass beiden Zahlen eine und dieselbe Classe M' der Gruppe $\mathfrak{M}'$ entspreche, in der Congruenz

$$\mu_1 \equiv \mu\varepsilon\omega' \text{ (mod. } \mathfrak{k}),$$

wo ε eine Einheit in $\mathfrak{o}$, und ω' eine in $\mathfrak{o}'$ enthaltene relative Primzahl zu $\mathfrak{k}$ bedeutet, deren Normen beide positiv sind.

Beweis. Ist $\mathfrak{m}' = \mathfrak{o}' - \mathfrak{o}\mu$ das Ideal in $\mathfrak{o}'$, welches dem Ideal $\mathfrak{o}\mu$ entspricht und folglich der Bedingung $\mathfrak{o}\mathfrak{m}' = \mathfrak{o}\mu$ genügt, so kann man, weil $\mathfrak{m}' + \mathfrak{k} = \mathfrak{o}'$ ist, eine Zahl μ' so wählen, dass $\mu' \equiv 0$ (mod. $\mathfrak{m}'$) und $\mu' \equiv 1$ (mod. $\mathfrak{k}$) wird (§. 2, 2^0); auch leuchtet ein, dass zugleich die Bedingung $N(\mu') > 0$ erfüllt werden kann (§. 6, 2^0). Dann ist $\mathfrak{o}'\mu'$ ein durch $\mathfrak{m}'$ theilbares Hauptideal in $\mathfrak{o}'$, weil $\mathfrak{o}'\mu' + \mathfrak{k} = \mathfrak{o}'$ ist, und folglich giebt es ein Ideal $\mathfrak{n}'$ in $\mathfrak{o}'$, welches der Bedingung $\mathfrak{m}'\mathfrak{n}' = \mathfrak{o}'\mu'$ genügt und folglich der inversen Classe M'^{-1} angehört. Hieraus folgt durch Multiplication mit $\mathfrak{o}$, dass $\mathfrak{o}\mu' = \mathfrak{o}\mathfrak{n}'\mu$, also μ' durch μ theilbar ist; setzt man $\mu' = \mu\nu$, so ist ν eine ganze Zahl von positiver Norm und relative Primzahl zu $\mathfrak{k}$, weil $\mu\nu = \mu' \equiv 1$ (mod. $\mathfrak{k}$) ist; zugleich wird $\mathfrak{o}\mu\nu = \mathfrak{o}\mathfrak{n}'\mu$, und folglich $\mathfrak{o}\mathfrak{n}' = \mathfrak{o}\nu$.

Wenn nun das dem Ideale $\mathfrak{o}\mu_1$ entsprechende Ideal $\mathfrak{m}'_1 = \mathfrak{o}' - \mathfrak{o}\mu_1$ derselben Classe M' angehört, wie $\mathfrak{m}'$, so ist auch $\mathfrak{m}'_1\mathfrak{n}'$ ein Hauptideal in $\mathfrak{o}'$, also $\mathfrak{m}'_1\mathfrak{n}' = \mathfrak{o}'\omega'$, wo ω' eine Zahl in $\mathfrak{o}'$ von positiver Norm und relative Primzahl zu $\mathfrak{k}$ ist. Multiplicirt man mit $\mathfrak{o}$ und berücksichtigt, dass $\mathfrak{o}\mathfrak{m}'_1 = \mathfrak{o}\mu_1$ und $\mathfrak{o}\mathfrak{n}' = \mathfrak{o}\nu$ ist, so folgt $\mathfrak{o}\mu_1\nu = \mathfrak{o}\omega'$, und hieraus $\mu_1\nu = \varepsilon\omega'$, wo ε eine Einheit in $\mathfrak{o}$ bedeutet, deren Norm $= +1$ sein muss, weil die Normen der Zahlen μ_1, ν, ω' positiv sind. Multiplicirt man mit μ, so ergiebt sich die zu beweisende Congruenz, weil $\mu\nu = \mu' \equiv 1$ (mod. $\mathfrak{k}$) und $\mathfrak{o}\mathfrak{k} = \mathfrak{k}$ ist.

Umgekehrt, wenn diese Congruenz, in welcher μ, μ_1, ε, ω' die in dem Satze angegebene Bedeutung haben, erfüllt ist, so folgt durch Multiplication mit $\nu\varepsilon^{-1}$ die Congruenz

$$\nu\mu_1\varepsilon^{-1} \equiv \omega' \text{ (mod. } \mathfrak{k}),$$

aus welcher hervorgeht, dass die ganze Zahl $\alpha' = \nu\mu_1\varepsilon^{-1}$, welche relative Prim-

zahl zu $\mathfrak{f}$ ist und eine positive Norm besitzt, der Ordnung $\mathfrak{o}'$ angehört, und folglich ist $\mathfrak{o}'\alpha'$ ein Hauptideal in $\mathfrak{o}'$. Da nun $\mathfrak{o}\nu = \mathfrak{o}\mathfrak{n}'$ und $\mathfrak{o}\mu_1\varepsilon^{-1} = \mathfrak{o}\mu_1 = \mathfrak{o}\mathfrak{m}_1'$ ist, so folgt $\mathfrak{o}(\mathfrak{o}'\alpha') = \mathfrak{o}(\mathfrak{n}'\mathfrak{m}_1')$, also auch $\mathfrak{o}'\alpha' = \mathfrak{n}'\mathfrak{m}_1'$ (§. 5, 1^0), mithin gehören die Ideale $\mathfrak{n}'$, $\mathfrak{m}_1'$ zu entgegengesetzten Classen, d. h. das dem Ideal $\mathfrak{o}\mu_1$ entsprechende Ideal $\mathfrak{m}_1'$ ist äquivalent mit $\mathfrak{m}'$, w. z. b. w.

Mit Hülfe dieses Satzes ist es leicht, die Anzahl m der in der Gruppe $\mathfrak{M}'$ enthaltenen Classen M' zu bestimmen. Wir bezeichnen mit $\psi(\mathfrak{f})$ die Anzahl aller der in $\mathfrak{o}$ enthaltenen Zahlen ω, welche incongruent in Bezug auf den Modul $\mathfrak{f}$ und zugleich relative Primzahlen zu $\mathfrak{f}$ sind; diese Anzahl ist (D. §. 163, 7.)

$$\psi(\mathfrak{f}) = N(\mathfrak{f}) \prod \left(1 - \frac{1}{N(\mathfrak{q})}\right),$$

wo das Productzeichen Π sich auf alle verschiedenen, in $\mathfrak{f}$ aufgehenden Primideale $\mathfrak{q}$ bezieht. Die Repräsentanten ω selbst können (nach §. 6, 2^0) immer so gewählt werden, dass sie positive Normen haben. Wenn eine dieser Zahlen (wie z. B. die Zahl 1) in $\mathfrak{o}'$ enthalten ist, so gehören auch alle mit ihr congruenten Zahlen der Ordnung $\mathfrak{o}'$ an, weil $\mathfrak{f}$ durch $\mathfrak{o}'$ theilbar ist; die Anzahl dieser nach $\mathfrak{f}$ incongruenten Zahlen ω' oder der zugehörigen Zahlclassen ist ebenfalls als bekannt anzusehen, sobald $\mathfrak{o}'$ gegeben ist, und soll mit $\psi'(\mathfrak{f})$ bezeichnet werden. Da $\mathfrak{o}'^2 = \mathfrak{o}'$ ist, so ist das Product aus je zwei Repräsentanten dieser Zahlclassen immer wieder einem solchen Repräsentanten congruent, und der Complex dieser $\psi'(\mathfrak{f})$ Repräsentanten hat daher den Charakter einer *Gruppe.* Multiplicirt man dieselben mit einer beliebigen in $\mathfrak{o}$ enthaltenen Zahl ω, welche relative Primzahl zu $\mathfrak{f}$ ist, so erhält man $\psi'(\mathfrak{f})$ incongruente Zahlen, welche ebenfalls relative Primzahlen zu $\mathfrak{f}$ sind, und deren Complex kurz mit (ω) bezeichnet werden soll; zwei solche Complexe (α), (β) sind (nach der in §. 8 angewendeten Schlussweise) entweder gänzlich verschieden, d. h. keine der in (α) enthaltenen Zahlen ist congruent mit einer der in (β) enthaltenen Zahlen, oder sie sind völlig identisch, d. h. alle durch den einen Complex vertretenen $\psi'(\mathfrak{f})$ Zahlclassen stimmen gänzlich mit den Zahlclassen des anderen Complexes überein. Es wird daher auch das System aller $\psi(\mathfrak{f})$ Repräsentanten in eine Anzahl solcher Complexe (ω) zerfallen, d. h. $\psi(\mathfrak{f})$ wird theilbar sein durch $\psi'(\mathfrak{f})$; wir betrachten zunächst aber nur alle diejenigen Complexe (ε), welche entstehen, wenn ε alle *Einheiten* des Gebietes $\mathfrak{o}$ durchläuft, deren Normen $= +1$ sind. Es sei s die Anzahl aller verschiedenen Complexe

$$(\varepsilon_1), (\varepsilon_2) \cdots (\varepsilon_s)$$

dieser Art, so bilden die in ihnen enthaltenen $s\psi'(\mathfrak{f})$ Repräsentanten offenbar wieder eine *Gruppe* im obigen Sinne; jede Zahl von der Form $\varepsilon\omega'$ ist einer und nur einer dieser Zahlen congruent, welche umgekehrt selbst in dieser Form enthalten sind. Ist nun μ eine in $\mathfrak{o}$ enthaltene relative Primzahl zu $\mathfrak{f}$, deren Norm positiv ist, und bezeichnet man mit $((\mu))$ den Complex der $s\psi'(\mathfrak{f})$ incongruenten, in den s Complexen $(\mu\varepsilon_1), (\mu\varepsilon_2) \cdots (\mu\varepsilon_s)$ enthaltenen Zahlen, so sind wieder zwei solche Complexe $((\mu))$ und $((\mu_1))$ entweder gänzlich verschieden, oder völlig identisch, und folglich besteht das System aller $\psi(\mathfrak{f})$ Repräsentanten ω aus einer Anzahl von solchen Complexen $((\mu))$; diese Anzahl muss aber nothwendig $= m$, d. h. gleich der Anzahl der verschiedenen, in der Gruppe $\mathfrak{M}'$ enthaltenen Idealclassen M' sein, weil nach dem obigen Satze je zwei Hauptidealen $\mathfrak{o}\mu$, $\mathfrak{o}\mu_1$ dieselbe Classe M' oder zwei verschiedene solche Classen entsprechen, je nachdem die beiden Complexe $((\mu))$, $((\mu_1))$ identisch oder verschieden sind. Mithin ist

$$\psi(\mathfrak{f}) = ms\psi'(\mathfrak{f}),$$

also

$$\frac{h'}{h} = m = \frac{\psi(\mathfrak{f})}{s\psi'(\mathfrak{f})}.$$

§. 10.

Umformung des Resultates.

Es ist nun noch von Wichtigkeit, die Anzahl s in bestimmter Weise darzustellen, und hierzu gelangt man mit Hülfe der in der Einleitung erwähnten Theorie der Einheiten von Dirichlet, welche ich zu diesem Zweck in etwas verallgemeinerter Form dargestellt habe (D. §. 166). Wir fragen zunächst: wie müssen zwei Einheiten ε, ε_0 von positiver Norm beschaffen sein, damit die oben mit (ε), (ε_0) bezeichneten Complexe identisch ausfallen? Offenbar ist hierzu erforderlich, dass $\varepsilon \equiv \varepsilon_0\omega' \pmod{\mathfrak{f}}$ sei, wo ω' eine der Ordnung $\mathfrak{o}'$ angehörende Zahl bedeutet; mithin muss $\varepsilon\varepsilon_0^{-1} \equiv \omega' \pmod{\mathfrak{f}}$, also $\varepsilon = \varepsilon'\varepsilon_0$ sein, wo $\varepsilon' = \varepsilon\varepsilon_0^{-1}$ eine der Ordnung $\mathfrak{o}'$ angehörende Einheit von positiver Norm bedeutet; und es leuchtet unmittelbar ein, dass diese Bedingung $\varepsilon = \varepsilon'\varepsilon_0$ auch hinreichend ist, dass sie also die Identität der Complexe (ε), (ε_0) zur Folge hat. Bezeichnet man daher, wie oben, mit

$(\varepsilon_1), (\varepsilon_2) \cdots (\varepsilon_s)$ die sämmtlichen s verschiedenen Complexe von der Form (ε), so ergiebt sich, dass man alle Einheiten ε der Ordnung $\mathfrak{o}$, und jede nur ein einziges Mal erhält, wenn man jede der s particulären Einheiten $\varepsilon_1, \varepsilon_2 \cdots \varepsilon_s$ mit allen Einheiten ε' der Ordnung $\mathfrak{o}'$ multiplicirt. Hieraus folgt zunächst, dass die s^{te} Potenz ε^s einer jeden Einheit ε in $\mathfrak{o}$ immer eine Einheit ε' in $\mathfrak{o}'$ ist, weil die s Complexe $(\varepsilon\varepsilon_1), (\varepsilon\varepsilon_2) \cdots (\varepsilon\varepsilon_s)$ nothwendig mit den Complexen $(\varepsilon_1), (\varepsilon_2) \cdots (\varepsilon_s)$, wenn auch in anderer Ordnung, übereinstimmen müssen, und weil folglich das Product

$$\varepsilon\varepsilon_1 \cdot \varepsilon\varepsilon_2 \cdots \varepsilon\varepsilon_s = \varepsilon^s \cdot \varepsilon_1\varepsilon_2 \cdots \varepsilon_s$$

von der Form $\varepsilon' \cdot \varepsilon_1\varepsilon_2 \cdots \varepsilon_s$ ist, wo ε' eine Einheit der Ordnung $\mathfrak{o}'$ bedeutet.

Wir müssen nun das Hauptresultat der Theorie der Einheiten kurz in Erinnerung bringen. Es sei ν die Gesammtanzahl der $(2\nu-n)$ reellen Wurzeln und der $(n-\nu)$ Paare von je zwei conjugirt-imaginären Wurzeln $a \pm bi$ der irreductibelen Gleichung $f(\theta) = 0$, aus welcher der Körper Ω entsprungen ist (§. 1); behält man von jedem Paare imaginärer Wurzeln nur die eine bei, so bleiben ν Wurzeln übrig, die mit

$$\theta', \theta'' \cdots \theta^{(\nu)}$$

bezeichnet werden mögen. Ist nun $\varepsilon = \varphi(\theta)$ eine beliebige Einheit des Körpers Ω, so soll durch das Symbol $l'(\varepsilon)$ der reelle Theil des Logarithmen von $\varphi(\theta')$ oder das Doppelte dieses reellen Theils bezeichnet werden, je nachdem θ' reell oder imaginär ist, und die Symbole $l''(\varepsilon), l'''(\varepsilon) \cdots l^{(\nu)}(\varepsilon)$ sollen die entsprechende Bedeutung in Bezug auf die anderen Wurzeln $\theta'', \theta''' \cdots \theta^{(\nu)}$ haben. Dann folgt aus $N(\varepsilon) = 1$, dass immer

$$l'(\varepsilon) + l''(\varepsilon) + \cdots + l^{(\nu)}(\varepsilon) = 0$$

ist. Es wird nun zunächst bewiesen (D. §. 166, 5.), dass es in jeder Ordnung $\mathfrak{o}'$ immer $(\nu - 1)$ von einander *unabhängige*, d. h. solche Einheiten $\rho'_1, \rho'_2 \cdots \rho'_{\nu-1}$ giebt, für welche die Determinante

$$\sum \pm\, l'(\rho'_1)\, l''(\rho'_2) \cdots l^{(\nu-1)}(\rho'_{\nu-1}),$$

welche wir zur Abkürzung mit

$$L(\rho'_1, \rho'_2 \cdots \rho'_{\nu-1})$$

bezeichnen wollen, einen von 0 verschiedenen (positiven) Werth besitzt. Lässt man nun $u_1, u_2 \cdots u_{\nu-1}$ alle ganzen rationalen Zahlen durchlaufen, so erhält man eine *Gruppe* R' von unendlich vielen in $\mathfrak{o}'$ enthaltenen Einheiten

$$\rho_1'^{u_1} \rho_2'^{u_2} \cdots \rho_{\nu-1}'^{u_{\nu-1}},$$

die sich durch Multiplication und Division reproduciren; je zwei verschiedenen Systemen von Exponenten entsprechen zwei verschiedene Individuen der Gruppe R'. Die Einheiten $\rho_1', \rho_2' \cdots \rho_{\nu-1}'$, welche eine *Basis* der Gruppe R' bilden, können offenbar ohne Aenderung von R' und $L(\rho_1', \rho_2' \cdots \rho_{\nu-1}')$ durch je $(\nu - 1)$ Einheiten ersetzt werden, welche aus R' so ausgewählt sind, dass die aus den zugehörigen $(\nu - 1)^2$ Exponenten u gebildete Determinante $= 1$ wird. Bezeichnet man mit $R'\alpha$ den Inbegriff aller Producte aus einer bestimmten Zahl α und jeder der in R' enthaltenen Einheiten, so sind zwei solche Complexe entweder gänzlich identisch, oder sie haben keine einzige Zahl gemeinschaftlich; das System *aller* Einheiten ε' der Ordnung $\mathfrak{o}'$ besteht (D. §. 166, 6.) aus einer *endlichen*, von R' abhängigen Anzahl r' solcher Complexe, woraus leicht folgt, dass $\varepsilon'^{r'}$ stets der Gruppe R' angehört. Hieraus ergiebt sich unmittelbar, dass unter allen Systemen von $(\nu - 1)$ unabhängigen Einheiten der Ordnung $\mathfrak{o}'$ auch solche Systeme $\rho_1', \rho_2' \cdots \rho_{\nu-1}'$ existiren, für welche die Determinante $L(\rho_1', \rho_2' \cdots \rho_{\nu-1}')$ einen *Minimumwerth* erhält; dann besteht das System aller Einheiten ε' der Ordnung $\mathfrak{o}'$ aus r' Complexen von der Form

$$R', R'\rho', R'\rho'^2 \cdots R'\rho'^{r'-1},$$

wo ρ' eine primitive Wurzel der Gleichung $\rho'^{r'} = 1$ bedeutet (D. §. 166, 7.). Ein solches System von $(\nu - 1)$ unabhängigen Einheiten $\rho_1', \rho_2' \cdots \rho_{\nu-1}'$ heisst ein *Fundamental-System* der Ordnung $\mathfrak{o}'$, und wir wollen zur Abkürzung den durch die Ordnung $\mathfrak{o}'$ vollständig bestimmten Quotienten

$$\frac{L(\rho_1', \rho_2' \cdots \rho_{\nu-1}')}{r'} = \mathrm{E}(\mathfrak{o}')$$

setzen*). Es würde sich, wie wir beiläufig bemerken, durch Betrachtungen, welche

*) In dem singulären Fall eines imaginären quadratischen Körpers ($n = 2$, $\nu = 1$) besteht R' aus der einzigen Einheit 1, r' bedeutet die endliche Anzahl aller in $\mathfrak{o}'$ enthaltenen Einheiten, und die Determinante $L(\varrho_1', \varrho_2' \cdots \varrho_{\nu-1}')$ ist durch 1 zu ersetzen.

den gleich folgenden sehr ähnlich sind (vergl. D. §. 161), auch leicht beweisen lassen, dass Zähler und Nenner dieses Quotienten sich mit einer und derselben ganzen rationalen Zahl multipliciren, wenn das Fundamental-System $\rho_1', \rho_2' \cdots \rho_{\nu-1}'$ durch ein *beliebiges* System von $(\nu - 1)$ unabhängigen Einheiten der Ordnung $\mathfrak{o}'$ ersetzt wird. Wir wollen nun beweisen, dass die in dem Verhältniss $h' : h = m$ auftretende Anzahl s der Complexe $\varepsilon'\varepsilon_1, \varepsilon'\varepsilon_2 \cdots \varepsilon'\varepsilon_s$, aus welchen das System aller Einheiten ε der Ordnung $\mathfrak{o}$ besteht,

$$= \frac{\mathrm{E}(\mathfrak{o}')}{\mathrm{E}(\mathfrak{o})}$$

ist.

Zu diesem Zwecke bezeichnen wir mit $\rho_1, \rho_2 \cdots \rho_{\nu-1}$ ein Fundamental-System von Einheiten der Ordnung $\mathfrak{o}$, mit R die zugehörige Gruppe der aus ihnen durch Multiplication und Division gebildeten Einheiten, und mit r die Anzahl der Complexe

$$R,\ R\rho,\ R\rho^2 \cdots R\rho^{r-1},$$

aus welchen das System aller Einheiten ε der Ordnung $\mathfrak{o}$ besteht, wo nun ρ eine primitive Wurzel der Gleichung $\rho^r = 1$ bedeutet. Unter diesen Einheiten ε befinden sich auch alle Einheiten ε' der Ordnung $\mathfrak{o}'$, weil $\mathfrak{o}'$ durch $\mathfrak{o}$ theilbar ist. Ist nun e ein bestimmter Index aus der Reihe $0, 1, 2 \cdots (\nu - 1)$, so giebt es unter allen denjenigen Einheiten von der Form

$$\sigma_e' = \rho^u \rho_1^{u_1} \rho_2^{u_2} \cdots \rho_e^{u_e},$$

welche, wie z. B. ρ_e^s, auch der Ordnung $\mathfrak{o}'$ angehören, mindestens eine

$$\rho_e' = \rho^{a^{(e)}} \rho_1^{a_1^{(e)}} \rho_2^{a_2^{(e)}} \cdots \rho_e^{a_e^{(e)}},$$

in welcher der letzte Exponent u_e seinen *kleinsten positiven Werth* $a_e^{(e)}$ erreicht, und es leuchtet ein, dass in jeder anderen Einheit σ_e' der letzte Exponent u_e nothwendig durch $a_e^{(e)}$ theilbar, also von der Form $a_e^{(e)} x_e$ sein muss, wo x_e eine ganze rationale Zahl bedeutet; es wird daher

$$\sigma_e' \rho_e'^{-x_e}$$

eine in $\mathfrak{o}'$ enthaltene Einheit von der Form σ'_{e-1}, oder $= 1$ sein, wenn $e = 0$ ist. In diesem letzteren Fall ist

$$\rho' = \rho^a,$$

und da $\rho^r = 1$ eine Einheit der Ordnung $\mathfrak{o}'$ ist, so muss r durch a theilbar, also

$$r = ar'$$

sein, und folglich ist ρ' eine primitive Wurzel der Gleichung $\rho'^{r'} = 1$. Hat man nun nach der obigen Vorschrift für jeden Index $e = 0, 1, 2 \cdots (\nu - 1)$ eine solche particuläre Einheit $\rho', \rho'_1, \rho'_2 \cdots \rho'_{\nu-1}$ der Ordnung $\mathfrak{o}'$ aufgestellt, so ergiebt sich, dass jede Einheit ε' der Ordnung $\mathfrak{o}'$, d. h. jede Einheit $\sigma'_{\nu-1}$, von der Form

$$\sigma'_{\nu-2}\rho'^{x_{\nu-1}}_{\nu-1} = \sigma'_{\nu-3}\rho'^{x_{\nu-2}}_{\nu-2}\rho'^{x_{\nu-1}}_{\nu-1} = \text{etc.},$$

also schliesslich von der Form

$$\varepsilon' = \rho'^{x}\rho'^{x_1}_1\rho'^{x_2}_2 \cdots \rho'^{x_{\nu-1}}_{\nu-1}$$

ist, wo $x, x_1, x_2 \cdots x_{\nu-1}$ ganze rationale Zahlen bedeuten, deren erste x auf die r' Werthe $0, 1, 2 \cdots (r' - 1)$ einzuschränken ist; umgekehrt leuchtet ein, dass alle Zahlen ε' von der vorstehenden Form auch wirklich Einheiten der Ordnung $\mathfrak{o}'$ sind. Da die Zahlen $a, a'_1, a''_2 \cdots a^{(\nu-1)}_{\nu-1}$ sämmtlich positiv sind, so ist auch ihr Product

$$A = aa'_1a''_2 \cdots a^{(\nu-1)}_{\nu-1}$$

positiv; nun ergiebt sich aus der Bildung der Einheiten $\rho'_1, \rho'_2 \cdots \rho'_{\nu-1}$, dass

$$L(\rho'_1, \rho'_2 \cdots \rho'_{\nu-1}) = \frac{A}{a}\, L(\rho_1, \rho_2 \cdots \rho_{\nu-1})$$

einen von 0 verschiedenen, positiven Werth hat; mithin bilden dieselben ein System von $(\nu - 1)$ unabhängigen Einheiten der Ordnung $\mathfrak{o}'$, ja sogar ein Fundamental-System, weil für jedes beliebige System von $(\nu - 1)$ Einheiten $\varepsilon'_1, \varepsilon'_2 \cdots \varepsilon'_{\nu-1}$ dieser Ordnung $\mathfrak{o}'$ offenbar $L(\varepsilon'_1, \varepsilon'_2 \cdots \varepsilon'_{\nu-1}) = p\, L(\rho'_1, \rho'_2 \cdots \rho'_{\nu-1})$ wird, wo p eine ganze rationale Zahl bedeutet. Bezeichnet man wieder mit R' die Gruppe aller Einheiten, welche aus $\rho'_1, \rho'_2 \cdots \rho'_{\nu-1}$ durch Multiplication und Division gebildet

werden können, so besteht das System aller Einheiten ε' der Ordnung $\mathfrak{o}'$ aus den r' verschiedenen Complexen

$$R', R'\rho', R'\rho'^2 \cdots R'\rho'^{r'-1}.$$

Da ferner oben $r = a r'$ gefunden ist, so ergiebt sich aus der vorhergehenden Gleichung

$$\mathrm{E}(\mathfrak{o}') = A\,\mathrm{E}(\mathfrak{o}).$$

Nun ist offenbar A die Anzahl aller derjenigen in $\mathfrak{o}$ enthaltenen Einheiten

$$\varepsilon_0 = \rho^v \rho_1^{v_1} \rho_2^{v_2} \cdots \rho_{\nu-1}^{v_{\nu-1}},$$

deren Exponenten den Bedingungen

$$0 \leqq v < a, \quad 0 \leqq v_1 < a_1' \cdots 0 \leqq v_{\nu-1} < a_{\nu-1}^{(\nu-1)}$$

genügen. Da ferner jede Einheit der Ordnung $\mathfrak{o}'$ die Form

$$\varepsilon' = \rho'^x \rho_1'^{x_1} \rho_2'^{x_2} \cdots \rho_{\nu-1}'^{x_{\nu-1}} = \rho^w \rho_1^{w_1} \rho_2^{w_2} \cdots \rho_{\nu-1}^{w_{\nu-1}}$$

hat, wo

$$\begin{aligned}
w_{\nu-1} &= a_{\nu-1}^{(\nu-1)} x_{\nu-1} \\
w_{\nu-2} &= a_{\nu-2}^{(\nu-1)} x_{\nu-1} + a_{\nu-2}^{(\nu-2)} x_{\nu-2} \\
&\cdots\cdots\cdots\cdots \\
w_1 &= a_1^{(\nu-1)} x_{\nu-1} + a_1^{(\nu-2)} x_{\nu-2} + \cdots + a_1' x_1 \\
w &= a^{(\nu-1)} x_{\nu-1} + a^{(\nu-2)} x_{\nu-2} + \cdots + a' x_1 + a x
\end{aligned}$$

ist, so kann man, wenn eine beliebige Einheit

$$\varepsilon = \rho^u \rho_1^{u_1} \rho_2^{u_2} \cdots \rho_{\nu-1}^{u_{\nu-1}}$$

der Ordnung $\mathfrak{o}$ gegeben ist, die Einheit ε', d. h. die Exponenten $x_{\nu-1}, x_{\nu-2} \cdots x_1, x$ stets und nur auf einzige Weise so wählen, dass die Zahlen

$$v = u - w, \quad v_1 = u_1 - w_1 \cdots v_{\nu-1} = u_{\nu-1} - w_{\nu-1}$$

den obigen Bedingungen genügen, dass also $\varepsilon\varepsilon'^{-1}$ eine der A Einheiten ε_0 wird;

jede Einheit $\mathfrak{e}$ der Ordnung $\mathfrak{o}$ lässt sich daher stets und nur auf eine einzige Weise in die Form $\mathfrak{e}'\mathfrak{e}_0$ setzen, wo $\mathfrak{e}'$ eine Einheit in $\mathfrak{o}'$, $\mathfrak{e}_0$ eine der obigen A Einheiten in $\mathfrak{o}$ bedeutet. Durchläuft $\mathfrak{e}'$ alle Einheiten der Ordnung $\mathfrak{o}'$, während $\mathfrak{e}_0$ constant bleibt, so erhält man einen Complex von unendlich vielen Einheiten $\mathfrak{e} = \mathfrak{e}'\mathfrak{e}_0$, und zwei solche Complexe, welche zwei verschiedenen Werthen von $\mathfrak{e}_0$ entsprechen, sind gänzlich verschieden von einander; mithin besteht das System aller Einheiten $\mathfrak{e}$ der Ordnung $\mathfrak{o}$ aus A solchen Complexen. Aber es ist oben gezeigt, dass die Anzahl dieser Complexe $= s$ ist; mithin ist $s = A$, d. h.

$$s = \frac{\mathrm{E}(\mathfrak{o}')}{\mathrm{E}(\mathfrak{o})},$$

w. z. b. w.

Hiernach nimmt das frühere Resultat für das Verhältniss der Classenanzahlen die folgende Form an

$$\frac{h'}{h} = m = \frac{\psi(\mathfrak{f})}{\psi'(\mathfrak{f})} \cdot \frac{\mathrm{E}(\mathfrak{o})}{\mathrm{E}(\mathfrak{o}')},$$

in welcher die Lösung unseres Problems nach der Methode von Gauss enthalten ist.

§. 11.

Zerlegbare Formen, welche den Idealen von beliebiger Ordnung entsprechen.

Bevor wir zu der Ableitung desselben Resultates nach der Methode von Dirichlet übergehen, wird es zweckmässig sein, mit einigen Worten den Zusammenhang zwischen den Idealen von beliebiger Ordnung und den zerlegbaren Formen des Körpers Ω zu besprechen.

Bilden die Zahlen $\omega_1, \omega_2 \cdots \omega_n$ eine bestimmte Basis der aus allen ganzen Zahlen des Körpers bestehenden Ordnung $\mathfrak{o}$, so wollen wir die n Basiszahlen

$$\omega'_\iota = k_1^{(\iota)}\omega_1 + k_2^{(\iota)}\omega_2 + \cdots + k_n^{(\iota)}\omega_n$$

der Ordnung $\mathfrak{o}'$ (§. 3) und die n Basiszahlen

$$\alpha'_\iota = a_1^{(\iota)}\omega'_1 + a_2^{(\iota)}\omega'_2 + \cdots + a_n^{(\iota)}\omega'_n$$

eines Ideals $\mathfrak{a}'$ in $\mathfrak{o}'$ (§. 4) immer so wählen, dass die Determinanten

$$\sum \pm k'_1 k''_2 \cdots k_n^{(n)} = (\mathfrak{o}, \mathfrak{o}') = k$$
$$\sum \pm a'_1 a''_2 \cdots a_n^{(n)} = (\mathfrak{o}', \mathfrak{a}') = N'(\mathfrak{a}')$$

werden, also *positive* Werthe erhalten.

Die sämmtlichen Zahlen des Ideals $\mathfrak{a}'$ sind von der Form

$$\alpha' = x_1\alpha'_1 + x_2\alpha'_2 + \cdots + x_n\alpha'_n,$$

wo die Variabelen $x_1, x_2 \cdots x_n$ alle ganzen rationalen Zahlen durchlaufen, und es ergiebt sich, genau wie für die Ideale in $\mathfrak{o}$ (D. §. 165), dass

$$N(\alpha') = N'(\mathfrak{a}')X$$

ist, wo X eine homogene Function $n$ten Grades der n Variabelen $x_1, x_2 \cdots x_n$ mit ganzen rationalen Coefficienten bedeutet, welche, wie aus §. 6 folgt, keinen gemeinschaftlichen Theiler haben; die Determinante dieser Form X (§. 1) ist

$$= D(\mathfrak{o}, \mathfrak{o}')^2 = Dk^2,$$

wo $D = \Delta(\Omega)$ wieder die Grundzahl des Körpers Ω bedeutet. Alle Formen X, welche allen verschiedenen Basen aller mit $\mathfrak{a}'$ äquivalenten Ideale entsprechen, sind äquivalent, d. h. sie gehen durch lineare Substitutionen mit ganzen rationalen Coefficienten, deren Determinanten $= +1$ sind, in einander über; jeder Idealclasse entspricht also eine bestimmte Formenclasse. Der Multiplication zweier Ideale $\mathfrak{a}'$, $\mathfrak{b}''$ der Ordnungen $\mathfrak{o}'$, $\mathfrak{o}''$ oder der Composition der sie enthaltenden Idealclassen A', B'' entspricht die Composition der zu den Idealen $\mathfrak{a}'$, $\mathfrak{b}''$ gehörigen Formen X, Y zu einer dem Ideale $\mathfrak{a}'\mathfrak{b}''$ entsprechenden Form Z, deren Determinante

$$= D(\mathfrak{o}, \mathfrak{o}'\mathfrak{o}'')^2$$

ist, und zugleich folgt hieraus die Composition der Formenclassen*).

*) Da, wie schon oben (§. 7, Anmerkung) bemerkt ist, Modulu existiren, welche keinem Ideale äquivalent sind, so ist, was ich hervorheben zu müssen glaube, in dem Obigen noch nicht die Theorie aller zerlegbaren Formen enthalten, welche den sämmtlichen Moduln eines Körpers Ω entsprechen.

Um die Rückkehr von diesen allgemeinen Untersuchungen zu dem Fall der *quadratischen* Körper und Formen zu erleichtern, füge ich noch folgende Bemerkungen hinzu, von deren Richtigkeit man sich leicht überzeugen wird (vergl. D. §§. 168 bis 170). Jede Wurzel einer irreductibelen quadratischen Gleichung ist von der Form $a + b\sqrt{c}$, wo c eine ganze rationale Zahl bedeutet, welche keine Quadratzahl und auch durch keine Quadratzahl ausser 1 theilbar ist; a und b sind rationale Zahlen, und b ist von 0 verschieden. Die Grundzahl D des quadratischen Körpers Ω, welcher aus der Zahl $a + b\sqrt{c}$ entspringt, ist $= c$ oder $= 4c$, je nachdem $c \equiv 1$, oder $c \equiv 2, 3 \pmod{4}$ ist; setzt man

$$\theta = \frac{D + \sqrt{D}}{2},$$

so bilden die Zahlen 1, θ eine Basis der Ordnung $\mathfrak{o}$, welche aus allen ganzen Zahlen

$$\omega = \frac{t + u\sqrt{D}}{2}$$

des Körpers besteht, wo t, u alle, der Bedingung $t \equiv Du \pmod{2}$ genügenden Paare von ganzen rationalen Zahlen zu durchlaufen haben. Jede Ordnung $\mathfrak{o}'$ ist dann von der Form $[1, k\theta]$, wo $k = (\mathfrak{o}, \mathfrak{o}')$ eine beliebige positive ganze rationale Zahl bedeutet; der Führer $\mathfrak{k}$ einer solchen Ordnung ist das Hauptideal $\mathfrak{o}k = [k, k\theta]$, und es ist $N(\mathfrak{k}) = k^2$. Setzt man, wenn p eine positive rationale Primzahl bedeutet,

$$(D, p) = 0, +1 \text{ oder } -1,$$

je nachdem $\mathfrak{o}p$ das Quadrat eines Primideals, das Product aus zwei verschiedenen Primidealen, oder selbst ein Primideal ist (vergl. D. §. 168), so ist

$$\psi(\mathfrak{o}k) = k^2 \prod \left(1 - \frac{1}{p}\right)\left(1 - \frac{(D, p)}{p}\right),$$

wo p alle verschiedenen in k aufgehenden Primzahlen durchläuft; da ferner jede Zahl der Ordnung $\mathfrak{o}'$ mit einer *rationalen* Zahl congruent ist in Bezug auf $\mathfrak{o}k$, so ist

$$\psi'(\mathfrak{o}k) = \varphi(k) = k \prod \left(1 - \frac{1}{p}\right),$$

und folglich

$$\frac{\psi(\mathfrak{o}k)}{\psi'(\mathfrak{o}k)} = k\prod\left(1-\frac{(D,\,p)}{p}\right).$$

Ist nun der Körper Ω imaginär, also D *negativ*, so ist (vergl. §. 10, Anmerkung)

$$\frac{\mathrm{E}(\mathfrak{o})}{\mathrm{E}(\mathfrak{o}')} = \frac{r'}{r},$$

wo r die Anzahl aller Einheiten in $\mathfrak{o}$, und r' die Anzahl aller Einheiten in $\mathfrak{o}'$ bedeutet. Die letztere Anzahl r' ist (wenn $\mathfrak{o}'$ von $\mathfrak{o}$ verschieden ist) immer $= 2$, und ebenso ist r immer $= 2$, ausgenommen die beiden Fälle $D = -3$, wo $r = 6$, und $D = -4$, wo $r = 4$ ist. Es ist daher im Allgemeinen

$$\frac{h'}{h} = m = k\prod\left(1-\frac{(D,\,p)}{p}\right),$$

aber dieses Product ist im Falle $D = -3$ durch 3, im Falle $D = -4$ durch 2 zu dividiren. Ist der Körper Ω reell, also D *positiv*, so ist $r = r' = 2$, und folglich

$$\frac{\mathrm{E}(\mathfrak{o})}{\mathrm{E}(\mathfrak{o}')} = \frac{\log\varepsilon}{\log\varepsilon'},$$

wo, wenn $k\sqrt{D} = \sqrt{D'}$ gesetzt wird,

$$\varepsilon = \frac{T+U\sqrt{D}}{2},\quad \varepsilon' = \frac{T'+U'\sqrt{D'}}{2}$$

die Fundamentaleinheiten der Ordnungen $\mathfrak{o}$, $\mathfrak{o}'$ bedeuten, und man erhält

$$\frac{h'}{h} = \frac{\log\varepsilon}{\log\varepsilon'}\cdot k\prod\left(1-\frac{(D,p)}{p}\right).$$

Was das Zeichen $(D,\,p)$ betrifft, so ist sein Werth $= 0$, wenn p in D aufgeht; ist $p = 2$ und D ungerade, also $D \equiv 1 \pmod{4}$, so ist $(D,\,p) = +1$ oder $= -1$, je nachdem $D \equiv 1 \pmod{8}$ oder $D \equiv 5 \pmod{8}$; ist endlich p ungerade, und D nicht theilbar durch p, so ist unter Anwendung der Bezeichnung von Legendre

$$(D,p) = \left(\frac{D}{p}\right).$$

Jeder Idealclasse in $\mathfrak{o}'$ entspricht nach den obigen Festsetzungen eine Classe von äquivalenten quadratischen Formen $ax^2 + bxy + cy^2$, deren constante Coefficienten a, b, c ganze rationale Zahlen *ohne gemeinschaftlichen Theiler* sind, und die gemeinschaftliche *Determinante* *) dieser Formen ist $D' = b^2 - 4ac = Dk^2$; wenn D negativ ist, so treten nur sogenannte *positive*, d. h. solche Formen auf, deren äussere Coefficienten a, c positiv sind. Umgekehrt entspricht eine bestimmte Classe von äquivalenten quadratischen Formen, deren Determinante D' keine Quadratzahl ist, immer einer und nur einer Idealclasse eines quadratischen Körpers Ω, und wenn $\mathfrak{o}'$ die Ordnung dieser Idealclasse bedeutet, so ist $D' = D(\mathfrak{o}, \mathfrak{o}')^2 = Dk^2$, wo D die Grundzahl von Ω ist. Mithin sind in den obigen Formeln die verschiedenen Sätze enthalten, welche sich auf die Anzahl der quadratischen Formen in verschiedenen Ordnungen und auf die Unterscheidung der eigentlich und uneigentlich primitiven Formen beziehen.

§. 12.

Methode von Dirichlet.

Wir wenden uns nun der zweiten Lösung desselben allgemeinen Problems zu, welche auf den von Dirichlet eingeführten Principien beruht. Durchläuft $\mathfrak{a}'$ alle Ideale der Ordnung $\mathfrak{o}'$, so convergirt die Reihe

$$S' = \sum \frac{s-1}{N'(\mathfrak{a}')^s}$$

für alle *positiven* Werthe von $(s-1)$; denn weil $N'(\mathfrak{a}') = N(\mathfrak{o}\mathfrak{a}')$ ist (§. 5, 1⁰), so bilden die Glieder dieser Reihe nur einen Theil der gleichfalls aus lauter positiven Gliedern bestehenden Reihe

$$S = \sum \frac{s-1}{N(\mathfrak{a})^s},$$

in welcher $\mathfrak{a}$ alle Ideale der Ordnung $\mathfrak{o}$ durchläuft, und deren Convergenz schon

*) Es ist wohl darauf zu achten, dass die hier im Sinne von §. 1 definirte Determinante das Vierfache der Zahl ist, welche von Gauss die Determinante der Form genannt wird, während der Begriff der (eigentlichen) Aequivalenz der Formen derselbe bleibt.

früher bewiesen ist (D. §. 167); übrigens ergiebt sich die Convergenz der Reihe S' auch aus den weiter unten folgenden Untersuchungen.

Unsere Hauptaufgabe besteht darin, den *Grenzwerth* zu ermitteln, welchem die Summe S' sich für unendlich kleine positive Werthe von $(s - 1)$ annähert. Zu diesem Zweck betrachten wir aber zunächst nur denjenigen Theil S'' der Reihe S', welcher allen, durch ein gegebenes Ideal $\mathfrak{m}'$ der Ordnung $\mathfrak{o}'$ theilbaren Hauptidealen $\mathfrak{a}'$ entspricht. Die allgemeine Form dieser Ideale $\mathfrak{a}'$ ergiebt sich auf die folgende Weise.

1) Jedes Ideal $\mathfrak{a}'$ ist von der Form $\mu\mathfrak{o}'$, wo μ eine in $\mathfrak{o}'$ enthaltene Zahl bedeutet, welche relative Primzahl zu dem Führer $\mathfrak{f}$ der Ordnung $\mathfrak{o}'$ ist.

2) Die Zahl μ muss in dem gegebenen Ideal $\mathfrak{m}'$ enthalten sein.

3) Die Norm der Zahl μ muss positiv sein.

Umgekehrt, wenn μ diese drei Bedingungen erfüllt, so ist $\mu\mathfrak{o}'$ jedenfalls eins von den Idealen $\mathfrak{a}'$, auf welche sich die Summe S'' erstreckt.

Bilden nun die Zahlen $\mu_1, \mu_2 \cdots \mu_n$ eine Basis des gegebenen Ideals $\mathfrak{m}'$, so ist zur Erfüllung der Bedingung 2) erforderlich und hinreichend, dass

$$\mu = m_1\mu_1 + m_2\mu_2 + \cdots + m_n\mu_n$$

sei, wo $m_1, m_2 \cdots m_n$ ganze rationale Zahlen bedeuten, und da $\mathfrak{m}'$ durch $\mathfrak{o}'$ theilbar ist, so ist jede solche Zahl μ auch in $\mathfrak{o}'$ enthalten. Aber sie soll zufolge 1) auch relative Primzahl zu $\mathfrak{f}$ sein. Bezeichnen wir nun wieder (wie in §. 9) mit $\psi'(\mathfrak{f})$ die Anzahl aller in $\mathfrak{o}'$ enthaltenen Zahlen ω', welche incongruent in Bezug auf $\mathfrak{f}$ und zugleich relative Primzahlen zu $\mathfrak{f}$ sind, so muss gleichzeitig

$$\mu \equiv \omega' \,(\text{mod. } \mathfrak{f}),\ \mu \equiv 0 \,(\text{mod. } \mathfrak{m}')$$

sein; da $\mathfrak{f} + \mathfrak{m}' = \mathfrak{o}'$ ist, so giebt es (nach §. 2, 2°) immer Zahlen μ, welche einem solchen Congruenz-Paar genügen, und sie bilden eine bestimmte Zahlclasse in Bezug auf den Modul $\mathfrak{f} - \mathfrak{m}'$, welcher offenbar $= \mathfrak{f}\mathfrak{m}'$ ist; denn da $\mathfrak{m}' > \mathfrak{o}\mathfrak{m}'$ ist, so ist $\mathfrak{f} - \mathfrak{m}'$ ein gemeinschaftliches Vielfaches der beiden relativen Primideale $\mathfrak{f}, \mathfrak{o}\mathfrak{m}'$, also auch ein Vielfaches ihres Productes $\mathfrak{f}\mathfrak{o}\mathfrak{m}' = \mathfrak{f}\mathfrak{m}'$, und umgekehrt ist $\mathfrak{f}\mathfrak{m}'$ ein gemeinschaftliches Vielfaches von $\mathfrak{f}$ und $\mathfrak{m}'$, weil $\mathfrak{m}' > \mathfrak{o}$, $\mathfrak{f} > \mathfrak{o}'$ und $\mathfrak{f}\mathfrak{o} = \mathfrak{f}$, $\mathfrak{o}'\mathfrak{m}' = \mathfrak{m}'$ ist. Die sämmtlichen Zahlen μ, welche den Bedingungen 1) und 2) genügen, bilden daher $\psi'(\mathfrak{f})$ verschiedene Zahlclassen (mod. $\mathfrak{f}\mathfrak{m}'$). Jede solche Zahlclasse besteht

aber, weil $k\mathfrak{m}' > \mathfrak{k}\mathfrak{m}'$ ist, aus $(\mathfrak{k}\mathfrak{m}', k\mathfrak{m}')$ verschiedenen Zahlclassen (mod. $k\mathfrak{m}'$), und folglich ist

$$c = \psi'(\mathfrak{k})(\mathfrak{k}\mathfrak{m}', k\mathfrak{m}')$$

die Anzahl der Zahlclassen (mod. $k\mathfrak{m}'$), aus welchen das System aller dieser Zahlen μ besteht. Es lässt sich leicht zeigen, dass diese Anzahl c von $\mathfrak{m}'$ unabhängig ist. In der That, aus

$$(\mathfrak{o}, \mathfrak{m}') = (\mathfrak{o}, \mathfrak{o}')(\mathfrak{o}', \mathfrak{m}') = (\mathfrak{o}, \mathfrak{o}\mathfrak{m}')(\mathfrak{o}\mathfrak{m}', \mathfrak{m}')$$

folgt

$$k N'(\mathfrak{m}') = N(\mathfrak{o}\mathfrak{m}')(\mathfrak{o}\mathfrak{m}', \mathfrak{m}'),$$

mithin, weil $N'(\mathfrak{m}') = N(\mathfrak{o}\mathfrak{m}')$ ist (§. 5, 1⁰), $(\mathfrak{o}\mathfrak{m}', \mathfrak{m}') = k$, also auch

$$(k\mathfrak{o}\mathfrak{m}', k\mathfrak{m}') = k,$$

weil offenbar für je zwei Moduln $\mathfrak{a}, \mathfrak{b}$ der Satz $(\eta\mathfrak{a}, \eta\mathfrak{b}) = (\mathfrak{a}, \mathfrak{b})$ gilt, sobald η eine von 0 verschiedene Zahl ist. Da ferner

$$(\mathfrak{o}, k\mathfrak{o}\mathfrak{m}') = (\mathfrak{o}, \mathfrak{k}\mathfrak{m}')(\mathfrak{k}\mathfrak{m}', k\mathfrak{o}\mathfrak{m}'),$$

also

$$(\mathfrak{k}\mathfrak{m}', k\mathfrak{o}\mathfrak{m}') = \frac{N(k\mathfrak{o}\mathfrak{m}')}{N(\mathfrak{k}\mathfrak{m}')} = \frac{N(k\mathfrak{o})}{N(\mathfrak{k})} = \frac{k^n}{N(\mathfrak{k})}$$

ist, so ergiebt sich

$$(\mathfrak{k}\mathfrak{m}', k\mathfrak{m}') = (\mathfrak{k}\mathfrak{m}', k\mathfrak{o}\mathfrak{m}')(k\mathfrak{o}\mathfrak{m}', k\mathfrak{m}') = \frac{k^{n+1}}{N(\mathfrak{k})},$$

und folglich ist

$$c = \frac{\psi'(\mathfrak{k})}{N(\mathfrak{k})} k^{n+1}$$

die Anzahl der fraglichen Zahlclassen in Bezug auf den Modul

$$k\mathfrak{m}' = [k\mu_1, k\mu_2 \cdots k\mu_n].$$

Wählt man aus jeder dieser Classen einen bestimmten Repräsentanten

$$a_1\mu_1 + a_2\mu_2 + \cdots + a_n\mu_n,$$

so werden alle Zahlen μ derselben Classe durch die Form

$$\mu = (a_1 + kz_1)\mu_1 + (a_2 + kz_2)\mu_2 + \cdots + (a_n + kz_n)\mu_n \qquad \text{(I)}$$

erzeugt, wenn $z_1, z_2 \cdots z_n$ alle ganzen rationalen Zahlen durchlaufen; und die sämmtlichen Zahlen μ, welche den Bedingungen 1) und 2) genügen, werden durch c solche lineare Formen erzeugt, und zwar jede nur einmal.

Von diesen Zahlen μ sind aber nur diejenigen beizubehalten, welche auch der dritten Bedingung

$$N(\mu) > 0 \qquad \text{(II)}$$

genügen. Umgekehrt erzeugt jede solche Zahl μ ein Hauptideal $\mu\mathfrak{o}'$ in $\mathfrak{o}'$, welches durch das gegebene Ideal $\mathfrak{m}'$ theilbar ist.

Aber es leuchtet ein, dass, wenn μ *alle* diese Zahlen durchläuft, jedes bestimmte, durch $\mathfrak{m}'$ theilbare Hauptideal $\mathfrak{a}'$ unendlich oft erzeugt wird. Ist nämlich μ_0 eine bestimmte von diesen Zahlen μ, so wird dasselbe Hauptideal $\mathfrak{o}'\mu_0$ offenbar durch alle, und nur durch die Zahlen μ erzeugt, welche von der Form $\mu = \varepsilon'\mu_0$ sind, wo ε' eine beliebige in $\mathfrak{o}'$ enthaltene Einheit (von positiver Norm) bedeutet. Um dies zu vermeiden, muss man den Zahlen μ neue Beschränkungen auferlegen. Zu diesem Zwecke kehren wir zu den Betrachtungen und Bezeichnungen des §. 10 zurück und erweitern die Bedeutung der dort erklärten ν Symbole $l', l'' \cdots l^{(\nu)}$. Ist $\omega = \varphi(\theta)$ eine *beliebige* von 0 verschiedene Zahl des Körpers Ω, und $\omega' = \varphi(\theta')$, so verstehen wir unter $l'(\omega)$ den reellen Theil des Logarithmen von

$$\frac{\omega'}{\sqrt[\nu]{N(\omega)}}$$

oder das Doppelte dieses reellen Theiles, je nachdem θ' eine relle oder imaginäre Wurzel der irreductibelen Gleichung $f(\theta') = 0$ ist; legt man ferner den Symbolen $l''(\omega), l'''(\omega) \cdots l^{(\nu)}(\omega)$ die entsprechende Bedeutung in Bezug auf die Wurzeln $\theta'', \theta''' \cdots \theta^{(\nu)}$ bei, so ist offenbar

$$l'(\omega) + l''(\omega) + \cdots + l^{(\nu)}(\omega) = 0.$$

Bilden nun $\rho_1', \rho_2' \cdots \rho_{\nu-1}'$ ein bestimmtes Fundamentalsystem $\mathfrak{R}$ von Einheiten der Ordnung $\mathfrak{o}'$, so wollen wir unter den *Exponenten* der Zahl ω in Bezug auf $\mathfrak{R}$ diejenigen völlig bestimmten reellen Werthe $x_1(\omega), x_2(\omega) \cdots x_{\nu-1}(\omega)$ verstehen, welche den ν Gleichungen

$$\begin{aligned}
l'(\rho_1')x_1(\omega) + l'(\rho_2')x_2(\omega) + \cdots + l'(\rho_{\nu-1}')x_{\nu-1}(\omega) &= l'(\omega)\\
l''(\rho_1')x_1(\omega) + l''(\rho_2')x_2(\omega) + \cdots + l''(\rho_{\nu-1}')x_{\nu-1}(\omega) &= l''(\omega)\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots&\cdots\cdots\\
l^{(\nu)}(\rho_1')x_1(\omega) + l^{(\nu)}(\rho_2')x_2(\omega) + \cdots + l^{(\nu)}(\rho_{\nu-1}')x_{\nu-1}(\omega) &= l^{(\nu)}(\omega)
\end{aligned}$$

genügen, deren letzte eine Folge der übrigen ist. Da $l'(\alpha\beta) = l'(\alpha) + l'(\beta)$ ist,

und dasselbe für die anderen Symbole l'', $l''' \cdots l^{(\nu)}$ gilt, so ist auch $x_1(\alpha\beta) = x_1(\alpha) + x_1(\beta)$, und dasselbe gilt auch für die anderen Exponenten $x_2, x_3 \cdots x_{\nu-1}$. Die Exponenten der Einheit

$$\varepsilon' = \rho'^{u} \rho_1'^{u_1} \rho_2'^{u_2} \cdots \rho'^{u_{\nu-1}}_{\nu-1},$$

wo ρ' wieder eine primitive Wurzel der Gleichung $\rho'^{r'} = 1$ bedeutet, sind offenbar die ganzen rationalen Zahlen $u_1, u_2 \cdots u_{\nu-1}$.

Ist nun μ_0 eine bestimmte der oben definirten Zahlen μ, d. h. eine Zahl, welche in einer der c linearen Formen (I) enthalten ist und zugleich der Bedingung (II) genügt, so sind die sämmtlichen Producte $\mu = \varepsilon'\mu_0$, welche den sämmtlichen Einheiten ε' der Ordnung $\mathfrak{o}'$ entsprechen, eben solche Zahlen, und alle diese Zahlen μ und keine anderen liefern, wie oben bemerkt, ein und dasselbe durch $\mathfrak{m}'$ theilbare Hauptideal $\mathfrak{a}' = \mathfrak{o}'\mu_0 = \mathfrak{o}'\mu$ der Ordnung $\mathfrak{o}'$. Da nun

$$x_1(\mu) = x_1(\mu_0) + u_1 \cdots x_{\nu-1}(\mu) = x_{\nu-1}(\mu_0) + u_{\nu-1}$$

ist, so kann man die ganzen rationalen Zahlen $u_1, u_2 \cdots u_{\nu-1}$ offenbar stets und nur auf eine einzige Art so wählen, dass

$$0 \leqq x_1(\mu) < 1 \cdots 0 \leqq x_{\nu-1}(\mu) < 1 \tag{III}$$

wird, und da hierbei der in ε' auftretende Factor ρ'^{u} seine sämmtlichen r' Werthe

$$1, \rho', \rho'^2 \cdots \rho'^{r'-1}$$

durchlaufen darf, so werden durch diese Bedingungen (III) aus dem System aller mit μ_0 associirten Zahlen $\mu = \varepsilon'\mu_0$ genau r' Zahlen μ herausgehoben, während alle übrigen ausgeschlossen werden. Lässt man daher μ alle diejenigen Zahlen durchlaufen, welche in den c linearen Formen (I) enthalten sind und zugleich den Bedingungen (II) und (III) genügen, so wird jedes durch $\mathfrak{m}'$ theilbare Hauptideal $\mathfrak{a}' = \mathfrak{o}'\mu$ der Ordnung $\mathfrak{o}'$ genau r' mal erzeugt, und folglich ist der von uns betrachtete Theil S'' der Summe S' identisch mit

$$\frac{1}{r'} \sum \frac{s-1}{N'(\mathfrak{o}'\mu)^s} = \frac{1}{r'} \sum \frac{s-1}{N(\mu)^s}.$$

Nun zerlegen wir diese Summe abermals in c Partialsummen, indem wir jedesmal die Beiträge derjenigen Zahlen μ zu einer Partialsumme sammeln, welche in

einer und derselben Linearform (I) enthalten sind und ausserdem den Bedingungen (II) und (III) genügen. Es sei t eine beliebige positive Grösse, und T die entsprechende Anzahl dieser Zahlen μ, für welche zugleich

$$N(\mu) \leqq t \tag{IV}$$

wird, so wollen wir beweisen, dass der Quotient $T:t$ mit unendlich wachsendem t sich einem endlichen Grenzwerthe nähert. Zu diesem Zwecke bezeichnen wir mit

$$h_1, h_2 \cdots h_n$$

ein System von reellen, *stetig* veränderlichen Grössen und betrachten die n homogenen linearen Functionen $\omega', \omega'' \cdots \omega^{(n)}$, welche aus

$$\omega = h_1\mu_1 + h_2\mu_2 + \cdots + h_n\mu_n$$

dadurch hervorgehen, dass die dem Körper Ω angehörigen Constanten $\mu_1, \mu_2 \cdots \mu_n$ durch die mit ihnen conjugirten Zahlen ersetzt werden, welche der Reihe nach den Wurzeln $\theta', \theta'' \cdots \theta^{(n)}$ der Gleichung $f(\theta) = 0$ entsprechen. Setzen wir auch in allen Fällen, wo die Werthe der Variabeln $h_1, h_2 \cdots h_n$ nicht sämmtlich rational sind, der Kürze wegen

$$\omega'\omega'' \cdots \omega^{(n)} = N(\omega),$$

so ist $N(\omega)$ eine homogene Function n^{ten} Grades von den Variabeln $h_1, h_2 \cdots h_n$. Wir beschränken nun zunächst die Variabilität dieser Grössen durch die Bedingung

$$0 < N(\omega) \leqq 1 \tag{V}$$

und definiren hierauf ein System von ν Functionen

$$l'(\omega), l''(\omega) \cdots l^{(\nu)}(\omega)$$

und aus diesem ein System von $(\nu-1)$ Functionen

$$x_1(\omega), x_2(\omega) \cdots x_{\nu-1}(\omega)$$

genau nach denselben Regeln, wie dies oben für den Fall geschehen ist, dass die sämmtlichen Variabeln $h_1, h_2 \cdots h_n$ rationale Werthe haben, und folglich ω eine Zahl des Körpers Ω ist. Hierauf beschränken wir die Variabilität der Grössen $h_1, h_2 \cdots h_n$ ferner durch die $(\nu-1)$ Bedingungen

$$0 \leqq x_1(\omega) < 1 \cdots 0 \leqq x_{\nu-1}(\omega) < 1. \qquad \text{(VI)}$$

Hierdurch, sowie durch die Bedingung (V), ist den Variabeln $h_1, h_2 \cdots h_n$ ein bestimmtes Gebiet G angewiesen, und zwar ist (vergl. D. §. 167) das über dieses Gebiet G ausgedehnte $n$fache Integral

$$g = \int dh_1\, dh_2 \cdots dh_n = \frac{\sigma L(\rho_1', \rho_2' \cdots \rho_{\nu-1}')}{\sqrt{\pm \Delta(\mu_1, \mu_2 \cdots \mu_n)}} = \frac{\sigma r' \mathrm{E}(\mathfrak{o}')}{k N'(\mathfrak{m}') \sqrt{\pm D}},$$

wo $\sigma = 2^{\nu-1}\pi^{n-\nu}$, im Falle $n = 2\nu$ aber $= (2\pi)^\nu$ ist; $\sqrt{\pm D}$ bedeutet die positive Quadratwurzel aus dem absoluten Werthe der Grundzahl D des Körpers Ω.

Die oben mit T bezeichnete Anzahl der in einer bestimmten Linearform (I) enthaltenen Zahlen μ, welche ausserdem den Bedingungen (II), (III), (IV) genügen, besitzt nun die folgende Bedeutung für das eben definirte Gebiet G. Setzt man

$$h_1 = \frac{a_1 + k z_1}{\sqrt[n]{t}}, \quad h_2 = \frac{a_2 + k z_2}{\sqrt[n]{t}} \quad \cdots \quad h_n = \frac{a_n + k z_n}{\sqrt[n]{t}},$$

so bringt jedes System von n ganzen rationalen Zahlen $z_1, z_2 \cdots z_n$, welchem eine solche Zahl μ entspricht, ein System von n reellen Werthen $h_1, h_2 \cdots h_n$ hervor, welches dem Gebiete G angehört; denn da $N(\omega)$ eine homogene Function n^{ten} Grades, jede der Functionen $x_1(\omega), x_2(\omega) \cdots x_{\nu-1}(\omega)$ aber eine homogene Function 0ten Grades von den Variabeln $h_1, h_2 \cdots h_n$ ist, so gehen die Bedingungen (II) und (IV) in die Bedingung (V), und die Bedingungen (III) in die Bedingungen (VI) über. Setzt man ferner

$$\frac{k}{\sqrt[n]{t}} = \delta; \quad \frac{a_1}{\sqrt[n]{t}} = h_1^0, \quad \frac{a_2}{\sqrt[n]{t}} = h_2^0 \quad \cdots \quad \frac{a_n}{\sqrt[n]{t}} = h_n^0,$$

so ist das durch $z_1, z_2 \cdots z_n$ hervorgebrachte, dem Gebiet G angehörende Werthsystem $h_1, h_2 \cdots h_n$ von der Beschaffenheit, dass die Grössen

$$\frac{h_1 - h_1^0}{\delta} = z_1, \quad \frac{h_2 - h_2^0}{\delta} = z_2 \quad \cdots \quad \frac{h_n - h_n^0}{\delta} = z_n$$

ganze rationale Zahlen werden; und umgekehrt leuchtet ein, dass jedes dem Gebiete G angehörende Werthsystem $h_1, h_2 \cdots h_n$, welches dieser letzten Bedingung genügt, rückwärts ein System von ganzen rationalen Zahlen $z_1, z_2 \cdots z_n$ und dadurch

eine Zahl μ der Linearform (I) hervorbringt, welche auch den Bedingungen (II), (III), (IV) genügt. Mithin ist T die Anzahl derjenigen dem Gebiete G angehörenden Werthsysteme $h_1, h_2 \cdots h_n$, für welche die Quotienten

$$\frac{h_1 - h_1^0}{\delta}, \frac{h_2 - h_2^0}{\delta} \cdots \frac{h_n - h_n^0}{\delta}$$

ganze rationale Zahlen werden. Wächst nun t über alle Grenzen, so wird δ unendlich klein, und aus dem Begriffe eines $n$fachen bestimmten Integrals ergiebt sich, dass

$$\lim (T\delta^n) = k^n \lim \left(\frac{T}{t}\right) = \int dh_1\, dh_2 \cdots dh_n = g$$

ist, mögen die Grössen $h_1^0, h_2^0 \cdots h_n^0$ von δ unabhängig sein oder nicht. Nach einem Fundamentalsatze von Dirichlet (D. §. 118) folgt hieraus, dass die auf alle Zahlen μ der einen Linearform (I) ausgedehnte Partialsumme

$$\frac{1}{r'} \sum \frac{s-1}{N(\mu)^s}$$

für alle positiven Werthe von $(s-1)$ convergirt und für unendlich kleine Werthe von $(s-1)$ sich dem Grenzwerthe

$$\frac{1}{r'} \lim \left(\frac{T}{t}\right) = \frac{g}{k^n r'} = \frac{\sigma \mathrm{E}(\mathfrak{o}')}{k^{n+1} N'(\mathfrak{m}') \sqrt{\pm D}}$$

nähert. Da derselbe von den Zahlen $a_1, a_2 \cdots a_n$, welche diese eine Linearform charakterisiren, gänzlich unabhängig ist, und da die Anzahl der Partialsummen, aus welchen die bis jetzt von uns betrachtete Summe S'' besteht,

$$= c = \frac{\psi'(\mathfrak{k})}{N(\mathfrak{k})} k^{n+1}$$

ist, so erhalten wir das Resultat

$$\lim S'' = \lim \sum \frac{s-1}{N'(\mathfrak{a}')^s} = \frac{\psi'(\mathfrak{k})}{N(\mathfrak{k})} \cdot \frac{\sigma \mathrm{E}(\mathfrak{o}')}{N'(\mathfrak{m}') \sqrt{\pm D}},$$

wo links die Summe über alle durch $\mathfrak{m}'$ theilbaren Hauptideale $\mathfrak{a}'$ der Ordnung $\mathfrak{o}'$ ausgedehnt ist.

§. 13.

Resultat dieser Methode.

Mit Hülfe des eben bewiesenen Satzes ist es leicht, unsere Aufgabe zu lösen. Nimmt man $\mathfrak{m}' = \mathfrak{o}'$, also $N'(\mathfrak{m}') = 1$, so ergiebt sich

$$\lim \sum \frac{s-1}{N'(\mathfrak{a}')^s} = \frac{\psi'(\mathfrak{k})}{N(\mathfrak{k})} \cdot \frac{\sigma E(\mathfrak{o}')}{\sqrt{\pm D}},$$

wo die Summe links über alle Ideale $\mathfrak{a}'$ ausgedehnt ist, welche der Hauptclasse O' der Ordnung $\mathfrak{o}'$ angehören.

Nun sei B' eine beliebige Ideal-Classe der Ordnung $\mathfrak{o}'$, und $\mathfrak{m}'$ ein bestimmtes Ideal der inversen Classe B'^{-1}. Durchläuft $\mathfrak{b}'$ alle Ideale der Classe B', während $\mathfrak{m}'$ unverändert bleibt, so werden die Producte $\mathfrak{b}'\mathfrak{m}'$ lauter Hauptideale $\mathfrak{a}'$ der Ordnung $\mathfrak{o}'$, welche durch $\mathfrak{m}'$ theilbar sind; und umgekehrt, ist $\mathfrak{a}'$ ein durch $\mathfrak{m}'$ theilbares Hauptideal der Ordnung $\mathfrak{o}'$, so giebt es (nach §. 5, 3⁰) ein und nur ein Ideal $\mathfrak{b}'$ in $\mathfrak{o}'$ von der Art, dass $\mathfrak{b}'\mathfrak{m}' = \mathfrak{a}'$ wird, und $\mathfrak{b}'$ muss nothwendig der Classe B' angehören, weil $\mathfrak{m}'$ ein Ideal der inversen Classe ist. Da ausserdem $N'(\mathfrak{b}'\mathfrak{m}') = N'(\mathfrak{b}')N'(\mathfrak{m}')$ ist, so ist die über alle Ideale $\mathfrak{b}'$ der Classe B' ausgedehnte Summe

$$\sum \frac{s-1}{N'(\mathfrak{b}')^s} = N'(\mathfrak{m}')^s \sum \frac{s-1}{N'(\mathfrak{a}')^s},$$

wo $\mathfrak{a}'$ alle durch $\mathfrak{m}'$ theilbaren Hauptideale der Ordnung $\mathfrak{o}'$ durchläuft. Hieraus ergiebt sich nach dem Schlusssatz des vorigen Paragraphen für unendlich kleine positive Werthe von $(s-1)$

$$\lim \sum \frac{s-1}{N'(\mathfrak{b}')^s} = \frac{\psi'(\mathfrak{k})}{N(\mathfrak{k})} \cdot \frac{\sigma E(\mathfrak{o}')}{\sqrt{\pm D}},$$

d. h. der Grenzwerth der über alle Ideale einer beliebigen Classe in $\mathfrak{o}'$ ausgedehnten Summe ist für jede Classe *derselbe*, und zwar offenbar von 0 verschieden.

Für den Specialfall, in welchem $\mathfrak{o}'$ das Gebiet $\mathfrak{o}$ aller ganzen Zahlen des Körpers Ω ist, ergiebt sich hieraus, weil $\mathfrak{f} = \mathfrak{o}$, $N(\mathfrak{f}) = \psi'(\mathfrak{f}) = 1$ wird, und weil die Anzahl h aller Ideal-Classen der Ordnung $\mathfrak{o}$ endlich ist (D. §. 164), das Resultat

$$\lim S = \lim \sum \frac{s-1}{N(\mathfrak{a})^s} = h\frac{\sigma E(\mathfrak{o})}{\sqrt{\pm D}},$$

wo die Summe über alle Ideale $\mathfrak{a}$ der Ordnung $\mathfrak{o}$ auszudehnen ist.

Durchläuft nun $\mathfrak{a}'$ alle Ideale der Ordnung $\mathfrak{o}'$, so durchläuft $\mathfrak{o}\mathfrak{a}'$ alle diejenigen Ideale der Ordnung $\mathfrak{o}$, welche relative Primideale zu dem Führer $\mathfrak{f}$ sind, und jedes nur ein einziges Mal. Da zugleich $N'(\mathfrak{a}') = N(\mathfrak{o}\mathfrak{a}')$ ist, so ist die über alle Ideale $\mathfrak{a}'$ der Ordnung $\mathfrak{o}'$ ausgedehnte Summe

$$S' = \sum \frac{s-1}{N'(\mathfrak{a}')^s} = \sum \frac{s-1}{N(\mathfrak{o}\mathfrak{a}')^s};$$

durchläuft aber $\mathfrak{p}$ alle verschiedenen in $\mathfrak{f}$ aufgehenden Primideale in $\mathfrak{o}$, so ist nach den allgemeinen Gesetzen der Theilbarkeit die über alle Ideale $\mathfrak{a}$ der Ordnung $\mathfrak{o}$ ausgedehnte Summe

$$\sum \frac{1}{N(\mathfrak{a})^s} = \prod \frac{1}{1-\frac{1}{N(\mathfrak{p})^s}} \cdot \sum \frac{1}{N(\mathfrak{o}\mathfrak{a}')^s} = \prod \frac{1}{1-\frac{1}{N(\mathfrak{p})^s}} \cdot \sum \frac{1}{N'(\mathfrak{a}')^s},$$

und folglich, weil

$$\prod \left(1-\frac{1}{N(\mathfrak{p})}\right) = \frac{\psi(\mathfrak{f})}{N(\mathfrak{f})}$$

ist,

$$\lim \sum \frac{s-1}{N'(\mathfrak{a}')^s} = \frac{\psi(\mathfrak{f})}{N(\mathfrak{f})} \lim \sum \frac{s-1}{N(\mathfrak{a})^s},$$

d. h.

$$\lim S' = \frac{\psi(\mathfrak{f})}{N(\mathfrak{f})} \lim S.$$

Da die rechte Seite einen endlichen Werth hat, so folgt zunächst, dass die Anzahl h' der Ideal-Classen in $\mathfrak{o}'$ endlich sein muss, weil oben für jeden Bestandtheil der

linken Seite, welcher einer einzelnen Classe entspricht, ein und derselbe von 0 verschiedene Grenzwerth gefunden ist. Setzt man diesen Werth und ebenso den Grenzwerth der rechten Seite ein, so ergiebt sich

$$h' \frac{\psi'(\mathfrak{k})}{N(\mathfrak{k})} \cdot \frac{\sigma E(\mathfrak{o}')}{\sqrt{\pm D}} = \frac{\psi(\mathfrak{k})}{N(\mathfrak{k})} \cdot h \frac{\sigma E(\mathfrak{o})}{\sqrt{\pm D}},$$

und hieraus

$$\frac{h'}{h} = \frac{\psi(\mathfrak{k})}{\psi'(\mathfrak{k})} \cdot \frac{E(\mathfrak{o})}{E(\mathfrak{o}')},$$

was mit dem in §. 10 nach der Methode von Gauss gefundenen Resultat übereinstimmt.


UNIVERSITY OF TORONTO
LIBRARY
PLEASE LEAVE THIS CARD
IN BOOK POCKET